Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

Humanitarian debate: Law, policy, action

New technologies and warfare

ICRC

INTERNATIONAL
REVIEW
of the Red Cross

Aim and scope

Established in 1869 the International Review of the Red Cross is a periodical published by the ICRC. Its aim is to promote reflection on humanitarian law, policy and action in armed conflict and other situations of collective armed violence. A specialized journal in humanitarian law, it endeavours to promote knowledge, critical analysis and development of the law and contribute to the prevention of violations of rules protecting fundamental rights and values. The Review offers a forum for discussion about contemporary humanitarian action as well as analysis of the causes and characteristics of conflicts so as to give a clearer insight into the humanitarian problems they generate. Finally, the Review informs its readership on questions pertaining to the International Red Cross and Red Crescent Movement and in particular on the activities and policies of the ICRC.

International Committee of the Red Cross

The International Committee of the Red Cross (ICRC) is an impartial, neutral and independent organization whose exclusively humanitarian mission is to protect the lives and dignity of victims of armed conflict and other situations of violence and to provide them with assistance. The ICRC also endeavours to prevent suffering by promoting and strengthening humanitarian law and universal humanitarian principles. Established in 1863, the ICRC is at the origin of the Geneva Conventions and the International Red Cross and Red Crescent Movement. It directs and coordinates the international activities conducted by the Movement in armed conflicts and other situations of violence.

International Review of the Red Cross
19, Avenue de la Paix
CH - 1202 Geneva
t +41 22 734 60 01
f +41 22 733 20 57
e-mail: review@icrc.org

Volume 94 Number 886 Summer 2012

INTERNATIONAL
REVIEW
of the Red Cross

Humanitarian debate: Law, policy, action

New technologies and warfare

INTERNATIONAL
REVIEW
of the Red Cross

CONTENTS

NEW TECHNOLOGIES AND WARFARE

Articles

How are new technologies changing modern warfare?

New technologies and the law

Volume 94 Number 886 Summer 2012

Volume 94 Number 886 Summer 2012

Comments and opinions

Reports and documents

Selected article on international humanitarian law

Books and articles

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

EDITORIAL: SCIENCE CANNOT BE PLACED ABOVE ITS CONSEQUENCES

In Greek mythology, the parable of Icarus illustrates the human desire to always go farther at the risk of colliding with the limitations of our nature. It also evokes the ambiguity of our thirst for knowledge and progress. Icarus and his father Daedalus are attempting to flee their enemy in Crete in order to reach Greece. Daedalus has the idea of fashioning wings, like those of birds, from wax and feathers. Intoxicated by flight, Icarus forgets his father's cautionary advice and flies too close to the sun. The heat melts the wax of his artificial wings, they crumble, and Icarus plunges into the sea and perishes.

The first successful motorized flight is credited to the Wright brothers. Their aeroplane, the *Flyer*, travelled several hundred metres on 17 December 1903, remaining in the air for less than one minute. The invention of the aeroplane then opened up enormous possibilities: the promise of eliminating distances between continents, countries, and people, facilitating trade and discovery of the world, as well as understanding and solidarity across nations.

While it took humankind thousands of years to make Icarus's dream a reality, it took only a decade to improve aeroplanes sufficiently for them to be used for military purposes, causing immeasurable human suffering. The first aerial bombardment reportedly took place on 1 November 1911 during the Italo-Turkish war in Tripolitania.[1] On 5 October 1914 a French aircraft shot down its German counterpart in the first aerial duel in history. A combination of new technologies soon improved bombing techniques and, in the decades that followed, torrents of incendiary bombs destroyed whole cities, such as Guernica, Coventry, Dresden, and Tokyo. Icarus' dream nearly led to humanity's downfall when the bombings of Hiroshima and Nagasaki ushered in the nuclear era. A little more than a century after the *Flyer* took off, drones piloted at a distance of thousands of kilometres are dropping their deadly payloads on Afghanistan, Pakistan, and Yemen. It is also becoming technically feasible to give drones the capacity to decide autonomously when to use their weapons.

Only a few generations back, people could expect to witness in their lifetimes one or perhaps two technological changes directly affecting their daily lives. Yet scientific and technical progress follows an exponential, not a linear curve. We have no doubt reached the point where the graph of that curve is becoming a nearly vertical line. With each passing day, science exerts more and more influence over societies, even those farthest from the centres of innovation. Yet science-fiction writer Isaac Asimov's observation is more timely than ever: 'The saddest aspect of

doi:10.1017/S1816383113000179

life right now is that science gathers knowledge faster than society gathers wisdom'.[2]

The dazzling scientific and technical progress of recent decades has given rise to unprecedented means and methods of warfare. Some of these new technologies (such as observation and combat drones) are already in use, while others (nanotechnologies, combat robots, and laser weapons) are still in the experimental and developmental stages. As well as the need for military capabilities on land, sea, and airspace, great armies are recognizing the need to have military capabilities in cyberspace.[3]

These developments herald the possibility of a quantum leap in the methods of waging war or using force outside of armed conflict, for some technologies are not just an extension of earlier ones (such as faster aircraft or more powerful explosives), they can profoundly change the ways in which wars are fought or even disrupt the international balance of power. After all, it was the control of mechanized warfare and blitzkrieg tactics that gave Germany a decisive advantage at the start of the Second World War.

It is difficult to define precisely the means and methods covered by the term 'new technologies', which is nonetheless the subject of impassioned debates among philosophers, legal scholars, and the military. Likewise, it appears futile to determine an exact date after which a technology can be considered new, since scientific and technical progress is, by definition, constantly evolving. The point here, rather, is to seek to identify general trends characterizing a number of technological innovations in the conduct of war – and, more broadly, the use of force – in recent years. What distinguishes drones, automated weapon systems, nanotechnology weapons, cyberwarfare, and the like from the conventional means and methods of warfare used up to now? In order to narrow the field of enquiry, the *International Review of the Red Cross* (the *Review*) has chosen to study, in particular, the technological innovations covered by one or more of the following three trends: first, the automation of weapon systems (both offensive and defensive) and, as a consequence, the delegation of a growing number of tasks to machines; second, progress with regard to the precision, the persistence,[4] and the reach of weapon systems; and, third, the capacity to use less and less physical and/or kinetic force to achieve equivalent or even larger effects.

Technologies that only yesterday were in the realm of science fiction could cause unprecedented catastrophes tomorrow, such as major technological accidents, or paralyze a country's health-care and supply systems by destroying computer networks in a cyberwar. Other recent developments, however, could not only limit

1 Sven Lindqvist, *Une histoire du bombardement* (A History of Bombing), La Découverte, Paris, 2012, p. 14.
2 Isaac Asimov and Jason A. Shulman, *Isaac Asimov's Book of Science and Nature Quotations*, Blue Cliff Editions, Weidenfeld & Nicolson, New York, 1988, p. 281.
3 The United States of America has had an operational cybercommand since May 2010. See US Department of Defense, 'US Cyber Command Fact Sheet', US Department of Defense Office of Public Affairs, 25 May 2010, available at: http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf (last visited July 2012).
4 For example, some drones have the capacity to remain in flight longer than aircraft, enabling them to conduct prolonged surveillance of an area.

civilian losses, but also spare the lives of combatants. Some of the technologies improve the precision of weapons or facilitate the gathering of intelligence on the nature of the target. In addition, the study of new technologies and war is not limited to military applications, but also puts new means at the disposal of humanitarian organizations, journalists, and the courts. For instance, communication and information technologies can alert the world to violations of the law, mobilize volunteers, and enable direct communication with victims of conflict. Progress in cartography and satellite imagery, as well as remote surgery, can also facilitate humanitarian action.

How are we to understand the accelerating technological advances in warfare? Must we view them as an unavoidable development and simply prepare ourselves to manage the consequences of their use? The German philosopher Hans Jonas, alluding to the unprecedented risks posed by nuclear physics and genetics, wrote: 'the collective practice in which we are engaged with leading-edge technology is still virgin territory for ethical theory . . . What can serve as a compass? Anticipation of the threat itself!'[5]

The development of new means and methods of warfare must not only go hand in hand with ethical thinking; it must also comply with the law. Under international humanitarian law, states have an obligation to determine the compatibility with international law of 'a new weapon, means or method of warfare' in the 'study, development, acquisition or adoption' phases.[6] Many means and methods of warfare have already been prohibited or their use regulated throughout history. For instance, blinding laser weapons were outlawed in 1995,[7] even before their appearance on the battlefield.

While science allows the automation of a growing number of tasks relating to the conduct of hostilities, assessing their legality from the standpoint of humanitarian law remains firmly within the human realm. Certain features of these new technologies, however, raise utterly unprecedented issues that make the legality of an attack more difficult to ascertain. In the first place, the possibility of having machines commit programmed acts of violence means delegating our capacity for judgement, the key element in the attribution of responsibility. Second, our growing use of (or dependence on) technology inevitably leads to greater vulnerability in terms of scientific uncertainties and risk of technical failures. To what degree can the extent – as yet uncertain – of the consequences of using nanotechnology weapons be taken into account? What degree of uncertainty is legally 'acceptable'?

5 Hans Jonas, *Le principe responsabilité : Une éthique pour la civilisation technologique*, Éditions du Cerf, Paris, 1990, preface, p. 13 [published in English as *The Imperative of Responsibility: In Search of an Ethics for the Technological Age*, University of Chicago Press, Chicago, 1985; the quotation has been translated from the French original].

6 Article 36 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I), 8 June 1977.

7 Protocol on Blinding Laser Weapons (Protocol IV to the 1980 United Nations Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects), Geneva, 13 October 1995.

Moreover, the growing use of technology in the conduct of hostilities raises complex issues of responsibility in view of the number of people – civilians and soldiers – involved in the process from the design to the use of the weapon in question. To whom should responsibility be ascribed for an illegal attack by a robot? How can fact-finding be adapted to the increasingly technical nature of war? Can a proven technical failure absolve the operator of 'fault'? In that case, should the machine's designer be held responsible?

In opening this issue, Peter Singer, a recognized expert in new combat technologies and the author of *Wired for War*,[8] sets out the terms of the debate in his interview. Next, several ethics, legal, scientific, and military experts focus on contemporary technological developments and their consequences, as well as the issues they raise for humanitarian action and law. Some of these contributions also portray varying national viewpoints, and the *Review* notably sought the Chinese and United States perspectives on cyberwar.

The contributions illustrate the deep ambiguity of new technologies in terms of their effects on war and its consequences. In what follows, we highlight some of the key issues and paradoxes raised by new technologies and discussed in this issue of the *Review*.

The blurring of the conventional concept of war

Like our societies, wars are also evolving as a result of new technologies. For the few countries that possess new technologies, the key development is undoubtedly the ability to commit acts of war without mobilizing conscripts, occupying territories, and conducting vast land operations, as was the case during the major wars of the twentieth century. Some technologies are nonetheless extremely complex and costly to develop. Few nations today are as yet capable of controlling their development and conducting remote operations.

Moreover, such methods of war do not fundamentally alter the cruel escalation of violence that often characterizes so-called asymmetrical conflicts between conventional forces and non-state armed groups. While the use of drones piloted at a distance of thousands of kilometres makes it possible to reach an enemy who cannot fight back, the enemy will often decide to compensate for such powerlessness by deliberately attacking civilians.

Far from being unaware of these distant wars, the populations of the countries that conduct this type of high-technology warfare are well informed about it. Yet the far-off enemy is often perceived mainly as a criminal and not as a belligerent whose rights and obligations are governed by humanitarian law.

It is possible that certain new technologies (for example, drones) could make the use of force on the territory of non-belligerent states less problematic by

8 P. W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, Penguin Books, New York, 2009.

making force protection issues moot, thereby eliminating traditional disincentives for attacking the enemy outside of the combat zone. This perceived lower barrier to entry could create the impression that the battlefield is 'global'. In this context, it must be noted that attacks conducted with drones without the requisite nexus to an armed conflict are governed not by humanitarian law (which allows for the use of lethal force against combatants, at least under certain conditions), but by international human rights law standards of law enforcement (which limit much more strictly the instances in which such force may be used).

The effects of some new technologies should lead to reflection on the meaning of the 'use of armed force' as the threshold of application of humanitarian law (*jus in bello*), particularly in the context of a cyberattack.[9] The same applies to the concept of an 'armed attack', which triggers the right of self-defence under the United Nations Charter (*jus ad bellum*). The 'low blows' and cyberattacks that states have engaged in so far seem to be more closely related to sabotage or espionage than to armed conflict. Would the rules governing (albeit sparsely and poorly) espionage and other hostile acts below the threshold of application of humanitarian law not be more appropriate to apply in such situations?

Recent conflicts show clearly that the deployment of troops and substantial military assets remains essential when the goal of an operation is to control territory. However, some new technologies allow those who possess them to strike their enemy with significant destructive effects – in both the real world and the virtual one – without deploying troops. A cyberattack means invading not an adversary's territory, but his virtual space, as it were. The concepts and images of conventional war must be reconsidered in order to avoid the blurring of existing legal categories of armed conflicts (international and non-international) and possibly weakening the protection that humanitarian law affords to victims.

Reach, precision, and moral distance

While for a long time increasing a weapon's reach meant reducing its precision, these two characteristics can now be reconciled through the use of drones, armed robots, and cybernetics. Increasing the reach of some new weapons avoids exposing troops directly to enemy fire. Above all, because of the weapons' precision, the payloads needed to destroy the military objective can be reduced and the harm done to civilians and their properties minimized. Having said that, the weapons often require very precise intelligence, which is difficult to gather at a distance.

Thus, the use of drones and robots turns out to be particularly suited to the use of force by countries concerned with saving the lives of their soldiers. In addition, it seems that keeping the operators of these new weapons far from the battlefield, in a familiar environment, significantly reduces their exposure to stress

9 See Cordula Droege, 'Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians', in this edition of the *Review*.

and fear and thus decreases errors due to emotional factors. However, the greater physical distance between the operator's location and the target also seems to increase the moral distance between the parties to the conflict. Thus, the proliferation of attacks conducted by remotely piloted drones fuels a debate about the so-called PlayStation mentality[10] that allegedly affects the moral judgement of the drone operators and exacerbates the crime-inducing phenomenon of dehumanization of the enemy in time of war. Those who counter this assertion point out that drone operators might in fact be more exposed morally than gunners or bomber pilots as a result of prolonged observation of their targets and the damage caused by the attacks.

This also raises the question of the mental picture that video-game players form of the reality of modern wars: usually, that of a lawless world in which anything is permitted in order to defeat the enemy. In cooperation with several National Red Cross Societies, the ICRC began a dialogue with players, designers, and producers of video games and aimed at the production of games incorporating the applicable law in time of armed conflict and presenting players with the same dilemmas as those facing combatants on today's battlefields.

Some observers see the development of autonomous weapon systems as having the potential to improve compliance with humanitarian law on the battlefield. A robot experiences neither fatigue nor stress, neither prejudice nor hatred, which are among the causes of crime in time of conflict. For now, however, it seems extremely difficult from a technical standpoint to give these weapons the capacity to make distinctions. As Peter Singer notes in this issue: 'A computer looks at an 80-year-old woman in a wheelchair the exact same way it looks at a T-80 tank. They are both just zeros and ones.' While fully autonomous weapon systems are not being used currently, some commentators are already calling for a total ban on autonomous weapons.[11] For its part, the ICRC emphasizes that the deployment of such systems 'raises a range of fundamental legal, ethical and societal issues which need to be considered before such systems are developed or deployed'.[12] Up to what point can people be 'taken out of the loop' when it comes to deciding whether or not to use lethal force?

10 Philip Alston describes the problem of the 'PlayStation mentality' in this way: 'Young military personnel raised on a diet of video games now kill real people remotely using joysticks. Far removed from the human consequences of their actions, how will this generation of fighters value the right to life? How will commanders and policymakers keep themselves immune from the deceptively antiseptic nature of drone killings? Will killing be a more attractive option than capture? Will the standards for intelligence-gathering justify a killing slip? Will the number of acceptable "collateral" civilian deaths increase?'. See Philip Alston and Hina Shamsi, 'A killer above the law', in *The Guardian*, 2 August 2010.

11 See Peter Asaro, 'On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making', and Noel E. Sharkey, 'The evitability of autonomous robot warfare', in this edition of the *Review*.

12 ICRC, 'International humanitarian law and the challenges of contemporary armed conflicts,' *Report of the 31st International Conference of the Red Cross and Red Crescent*, ICRC, Geneva, October 2011, p. 39, available at: http://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf (last visited July 2012).

Damage

The progress made in terms of targeting precision must be placed alongside another, opposite trend: the difficulty of limiting the temporal and spatial effects of some new weapons. This trend is, of course, not new; we know, for example, of the indiscriminate effects of atomic weapons, which extend well beyond the point of impact. But the introduction of nanotechnologies into weapon systems and the use of cyberattacks bring these issues to the fore again. How can the temporal and spatial effects of the use of nanotechnologies be taken into account in the calculation of proportionality when these effects are as yet largely unknown? What degree of scientific uncertainty would allow us to determine that the use of these materials would run counter to the precautionary principle? Can we measure the impact that an attack launched in the virtual world may have on the real world? Indeed, taking into account all these unknowns, the consequences that might not be 'expected'[13] are becoming more and more numerous.

Moreover, some new means and methods of warfare, such as microwave weapons and cyberattacks, often seek to destroy information. Should information now be regarded as a civilian object under humanitarian law and its destruction as damage to civilian object? Today, in fact, only physical harm is included in the definition of damage. In a world increasingly dependent on information, the destruction of the banking and medical data of a country's citizens would have drastic repercussions; in the view of some, this calls for a redefinition of the concept of a protected civilian object. The ICRC's position in this discussion aims to be clear and pragmatic: 'If the means and methods of cyber warfare produce the same effects in the real world as conventional weapons (such as destruction, disruption, harm, damage, injuries or death), they are governed by the same rules as conventional weapons'.[14]

Information and transparency

The technological innovations that we have witnessed in recent decades seem to point to two opposite conclusions in terms of transparency and access to information. On the one hand, there is still little transparency concerning the real or possible consequences of the use of some new weapons. If they are used in secret operations, the public will have only scant knowledge of the impact of these weapons.

On the other hand, the use of new technologies makes it possible to film and record military operations and to reveal possible war crimes. This may be done

13 Pursuant to Arts 51(5)(b) and 57(2)(a)(iii) of Additional Protocol I, an indiscriminate attack is 'an attack which may be *expected* to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated' (emphasis added).

14 Cordula Droege, 'No legal vacuum in cyber space', ICRC, Interview, 16 August 2011, available at: http://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm (last visited November 2012).

by armies themselves (in order to produce an 'after-action report') or by international and non-governmental organisations. For example, the use of satellite imagery has already facilitated investigations into possible violations of the law in the Gaza Strip, Georgia, Sri Lanka, and Sudan.[15] In recent years, many crimes have also been exposed in videos taken by soldiers themselves!

Finally, technical progress has always made for improvements in medicine and humanitarian efforts. Nowadays the use of new communication and geolocation technologies can make it easier to identify needs, restore family links after a crisis, and track population displacements in remote corners of the world.[16]

Our responsibilities

While technology enables us to delegate a number of tasks, and even sometimes to avoid making mistakes, it in no way allows us to delegate our moral and legal responsibility to comply with the applicable rules of law. The use of new technologies in the conduct of war may, however, make it more complex to attribute responsibility when violations of humanitarian law occur, for two reasons. First, with some new technologies, there are technical difficulties in identifying those responsible. The best example of the growing complexity of the identification process, and of the increased technical skills that it requires, is the use of cyberwarfare. One of the features of attacks in cyberspace is their anonymity and the difficulty of locating their origin. Likewise, the automation of some computer-directed missile-launch sequences weakens the concept of responsibility. Second, the delegation of some military tasks to 'smart' machines has the effect of increasing the number of people potentially involved in the building, acquisition, and use of the machines, thereby complicating the chain of responsibility. If we look beyond just the application of the law in time of conflict, responsibility would lie not only with the military chain of command or among the combatants who are or will be using these weapons on the battlefield – it would also lie with the scientists and builders who develop these new technologies and the political authorities and enterprises that commission them.

States have an obligation to ensure that the use of new weapons and new means and methods of warfare is consistent with the rules of humanitarian law. However, civil society also has an important role to play. By reporting on the consequences of weapons and eliciting a debate about their legality, it helps to shape a real international 'public conscience', as referred to in the Martens Clause:

> In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the

15 See Joshua Lyons, 'Documenting violations of international humanitarian law from space: a critical review of geospatial analysis of satellite imagery during armed conflicts in Gaza (2009), Georgia (2008), and Sri Lanka (2009)', in this edition of the *Review*.

16 See, for example, Patrick Meier's article, 'New information technologies and their impact on the humanitarian sector', in *International Review of the Red Cross*, Vol. 93, No. 884, 2011, pp. 1239–1263.

> principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience.[17]

The International Court of Justice (ICJ) has emphasized the importance of this clause in its Advisory Opinion on the *Legality of the Threat or Use of Nuclear Weapons.*[18]

For many years, the ICRC – now joined by many non-governmental organizations – has contributed to the formation of this 'public conscience'. Faced with the rapid and ongoing evolution of weapons, the ICRC published a *Guide to the Legal Review of New Weapons, Means and Methods of Warfare*,[19] and is contributing actively to the development of new international rules regulating the use of weapons. The most recent example of a treaty with such purpose is the Convention on Cluster Munitions of 30 May 2008.

***

'Science Finds, Industry Applies, Man Conforms': contrary to the slogan of the 1933 Chicago World's Fair, we are not condemned to be helpless witnesses to technological development. Scientific and technological development does not necessarily mean progress, and the decision to apply an invention for military purposes must give rise to an in-depth study on the impact of the use of the invention, including the positive and negative consequences thereof. Likewise, each decision to produce, buy, and ultimately use one or another technological innovation for military ends involves a political and civic responsibility, one that is all the more important in that it has direct repercussions for human lives. The consequences of armed conflicts are not 'virtual'. The debate that the use of some new technologies for military purposes solicits within civil society and in scientific, military, and political communities should be seen as a positive development: it is a sign of our questioning the compatibility of these new weapons with our legal and moral principles.

Just as the Wright brothers probably did not foresee the full potential of the aeroplane, so the military possibilities offered by new technologies (and the unprecedented combinations thereof) remain largely unknown. However, it is essential to anticipate the consequences that their use may entail. The ICRC, which

17 Art. 1(2) of Additional Protocol I. See also the preamble to the 1907 Hague Convention (IV) respecting the Laws and Customs of War on Land and the preamble to the 1899 Hague Convention (II) with Respect to the Laws and Customs of War on Land.

18 The ICJ was of the opinion that the 'continuing existence and applicability' of the Martens Clause was 'not to be doubted' (para. 87), and that it had 'proved to be an effective means of addressing the rapid evolution of military technology' (para. 78). It also noted that the clause represented 'the expression of the pre-existing customary law' (para. 84). See ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996, ICJ Reports 1996, p. 226.

19 ICRC, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare*, ICRC, Geneva, 2007, available at: http://www.icrc.org/eng/resources/documents/publication/p0902.htm (last visited July 2012). See also Kathleen Lawand, 'Reviewing the legality of new weapons, means and methods of warfare', in *International Review of the Red Cross*, Vol. 88, No. 864, 2006, pp. 925–930.

has been present in the world's conflicts for a century and a half, can unfortunately attest to that: contrary to the illusions about an unending 'progress' that people nourished at the start of the twentieth century, history has shown that science cannot be placed above its consequences.

Vincent Bernard
Editor-in-Chief

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

Interview with Peter W. Singer*

Director of the 21st Century Defense Initiative at the Brookings Institution.

Peter W. Singer is Director of the 21st Century Defense Initiative at the Brookings Institution in Washington, D.C. He is the author of three award winning books, Corporate Warriors: The Rise of the Privatized Military Industry, Children at War, *and* Wired for War: The Robotics Revolution and Conflict in the 21st Century.[1] *He has served as a consultant with groups that range from the US military and FBI to human rights organizations.*

In this interview, Peter Singer explains to what extent and how new technologies change the way we think about going to war and the way we conduct war, as well as how they will impact the work of humanitarian actors. He shares his vision for the future, analyzing both the ethical and legal challenges that access to new advanced technologies poses and the opportunities it offers.

: : : : : : :

Tell us a bit about your personal background. How and why did you come to work on this topic?

As I write in the opening of my book *Wired for War*, when I think back on my childhood it is a mix of playing with the bits and pieces of my family's military history combined with science fiction. Like a lot of other little boys, if I picked up a stick, within a couple of seconds that stick was transformed either into a machine gun that I was going to defend the neighbourhood against the Nazis with, or it was a light sabre I was going to use to defeat Darth Vader. I remember taking my grandfather's old medals and pinning them to my pyjamas, and taking a model of the jet that my uncle had flown in Vietnam and using it to protect Legoland. But

* This interview was conducted in Washington D.C. on 29 April 2012 by Vincent Bernard, Editor-in-Chief of the *International Review of the Red Cross*, Mariya Nikolova, Editorial Assistant, and Mark Silverman, Head of Public and Congressional Affairs, ICRC Washington.

doi:10.1017/S1816383112000677

then, also like a lot of other kids, there are artefacts of science fiction that are all around those memories so, yes, I might have been wearing my grandfather's old World War II medals on my pyjamas, but I was jumping into a bed that had Star Wars sheets.

The writer John Keegan once said in his book *Six Armies in Normandy*,[2] 'I grew up in this milieu of military history and war, it is not polite to say so, but this is a reality.' And I think that there was something in this. Now, I need to be very clear. My experience was then shaped by later connections to the real side of war. I remember going to Bosnia as part of a UN research team, and going into Mostar and seeing how the pictures in my grandfather's old books had seemingly come to life. The old pictures in my grandfather's book, however, did not come with the smell, with the feeling and emotions in the air amidst real war . . . When you read a book, you do not have to think about where to step next to avoid landmines, or try to walk where the locals walk to avoid stepping on one.

So my point here is that one shaping force for me was the historicized, fictionalized side of war that many of us grow up with and which was then tempered by real world experiences. The other shaping force is that I am an academic who works on public policy issues, and I have continually been struck by the disconnect between how we think the world works and how it actually works. This has been a hallmark of my own studies.

For example, when I was in Bosnia, I came across an American company that was working as a private military contractor. This concept did not exist in our studies of war and politics back then, and yet there was the company. When I proposed to write a dissertation on the concept, a professor at Harvard said I should quit graduate school and instead become a screenwriter, having thought about exploring such a silly, fictional idea. That dissertation became my book *Corporate Warriors*, and we have seen all the issues that have arisen since then from non-state (corporate) actors' involvement in the battlefield.

Similarly, while doing research on private militaries, I came to examine the case in West Africa, where we saw a kind of war that no one thought should exist. On one hand, there was a government hiring a private company to serve as its military, and on the other side a corporate force fighting against a rebel force that was primarily made up of abducted children. Neither side fit the model of how we understood war, and yet there they were. That became the basis of the next book I wrote, *Children at War*. Again, I had a similar experience with one professor who said that she did not believe the child soldiers even existed. Today, of course, this notion sounds silly, but in the early 1990s people thought that way.

My most recent book linked back to this notion of exploring new actors, but also tried to open people's eyes to what is happening. In it, I look at robotics and

1 See Peter W. Singer, *Corporate Warriors: The Rise of the Privatized Military Industry*, updated edn, Cornell University Press, New York, 2007; *Children at War*, University of California Press, Berkeley C.A., 2006; and *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, Penguin Books, New York, 2009.

2 See John Keegan, *Six Armies in Normandy: From D-Day to the Liberation of Paris; June 6–Aug. 5, 1944*, revised edn, Penguin Books, New York, 1994.

all the very real implications that it has had on combat and the political and ethical issues beyond the battlefield. I have already had experiences with it similar to those that I had with the dissertation and first book. People, both those in the senior defence leadership who were themselves not aware that their militaries were using the technology *and* those in humanitarian organizations who still see robotics as science fiction technology, have a response to it that has a tint of 'too little, too late'.

What are these new technologies bringing to the battlefields? What do robotics change in the way we see war today?

There is this notion – sometimes within the defence establishment – of a 'revolutionary technology', and we frequently misunderstand the idea. A revolutionary technology is a game-changing technology on a historic level. It is technology like gunpowder, or the steam engine, or the atomic bomb.

Now, let me be very clear. These technologies do not solve all the problems of war. Too often they are discussed as if they were silver-bullet solutions. Donald Rumsfeld, for instance, talked about how computer network technology might 'lift the fog of war'. We also frequently see new technology described in the same way in the humanitarian community, that is, as if it might make war safer or cleaner. And this is nothing new. The poet John Donne predicted in 1621 that cannons would mean that wars would 'come to quicker ends than heretofore, and the great expense of blood is avoided'.[3] We have seen how better cannon did not make war less bloody, or less expensive. And views have not changed today, when many now talk about robots as if they will solve the ethical issues of war.

Revolutionary technologies are game-changers, not because they solve all problems, but because they force new questions upon us that a generation earlier people did not imagine we would be asking ourselves, or our respective organizations or nations. Some of these questions are questions of what was possible a generation ago versus what is possible today.

Just recently, I was speaking with a two-star general about the capability of being able to watch what's happening across the battlefield up close and personal, but with a plane that's flown from 7,000 miles away. He never even imagined he'd be able to have that capability when he was a younger officer, and now he's commanding an entire force with that capability. We see that opening up of new possibilities on the humanitarian side, and the idea that non-governmental organizations (NGOs) might have the very same capability to watch and document crimes without sending people into harm's way.

However, revolutionary technologies also come with questions of what is proper, questions that were never imagined previously; issues of right and wrong that were never explored previously. A commander today may be able to watch what is happening on the battlefield from 7,000 miles away, but what does that mean for his unit structure, the tactics he uses, the doctrine he uses, when and where he utilizes force, and under what rules and conditions? In the same way that the

3 John Donne, Sermon CXVII, Preached at St. Paul's upon Christmas Day, 1621, John 2:8.

capability of a humanitarian organization watching an atrocity from afar may be a real capability, watching a battlefield from afar also raises questions on everything from obligation of those watching to respond, to whether the notion of 'costless war' also applies to costless humanitarian operations, and whether with the potential to lower the risk to humanitarian workers just by watching from afar, there is also a cheapening of the life of those on the ground.

I am of the opinion that certain technologies are game-changers, and robotics is in that category. When I interviewed people in the field for what they thought the historical parallels were to robotics today, their answers were illustrative. The engineers said unmanned systems, or robotics, are like the horseless carriage in 1910. Even the terms used to describe them – 'horseless' carriage and 'unmanned' system – demonstrate that we still like to wrap our heads around what something is *not*, rather than what it is. If we choose to draw a parallel between the horseless carriage and robotics, we can also see how robotics may end up impacting our society, the conduct of war, and issues of law. There was no such thing as 'traffic laws', for example, before the horseless carriage.

The parallel that others – like Bill Gates, the founder of Microsoft, for instance – draw is with the computer around 1980. The computer in 1980 was a big bulky device, which could only perform a limited set of functions. It was developed by the military and the military was the main customer for it and researcher on it. Today, computers are so ubiquitous that we do not even call them computers anymore. I drive a car with over 100 computers in it. Again, if we choose to use that parallel, we need to consider all the implications of entering the information age. Who, back in 1980, would have thought that a computer would be capable of leading to things like cyber warfare, or deep challenges to personal privacy?

The final parallel, which some of the scientists worry about, is with the atomic bomb, in the 1940s. The parallel, they say, is that much like nuclear physics in the 1940s, robotics and artificial intelligence are today such a cutting-edge field that all the best minds are drawn to it. If, as a scientist, you wanted to work on what was important in the 1940s you were drawn towards nuclear physics. Today, you are drawn towards robotics and artificial intelligence. But scientists, as well as others, also worry about what all of that means.

Scientists today worry about an equivalent of what played out with the people behind *the Manhattan Project*,[4] where they created a game-changing technology (the atomic bomb), and then asked 'What just happened?' It is deeply ironic that many of the same people who built the atomic bomb went on to create the modern arms control movement. But the genie was already out of the bottle. And there are obvious parallels here to robotics, too. Only, in this case, the genie literally may get up and walk out of the bottle.

4 Editor's note: 'Manhattan Project' is the code name of a secret US government research and development project that built the first atomic bomb during the Second World War.

In your book, you write that war is nevertheless still waged by humans on humans' behalf. It is also still about human suffering, about loss of human lives and consequences for human beings. What will robotics change in the way we think about going to war or about the way we conduct war?

Robotics is having an impact on the psychology and the politics of war. But no matter the technology, war is a human endeavour. And that holds true now even with this advanced technology. The technology is shaping how we, in the public, and especially our leaders, look at and interpret war, and decide when it makes sense and when it does not, and what its likely or real costs are.

Where I think we see this impact most today is in the connection amongst the technology of robotics and democracies and war. No longer, in most democracies, is there conscription. We do not have declarations of war any more. The last time, for example, the US Congress formally declared war was in 1942, against the minor members of the Axis powers. We do not buy war bonds, or pay war taxes any more. During the Second World War, for example, the US public personally bought, that is personally invested in, over $180 billion worth of war bonds. In fact, people were so invested in the war effort that if one raised over $200,000, one got to name your own ship. In the past ten years of war, by comparison, the US public bought zero dollars' worth of war bonds, and instead of a war tax, the richest 4 per cent received a tax break. And now we have a technology that enables us to carry out acts of what we previously would have thought of as war, without having to wrestle with some of the potential political costs of sending a son or daughter into harm's way.

So the barriers to war in our societies were already lowering before this technology came along. This new technology, though, may take those barriers to the ground. This is not just a notion of political theory. It relates to our oldest ideals of how democracies are better, more honourable, more thoughtful when it comes to war. It relates to the connection between the public and its wars. We can see this in a variety of operations right now. For instance, there have been more than 350 air strikes conducted into Pakistan that were not voted on by Congress. Such strikes are not conducted by the US military, but by covert intelligence operations, and lack the level of transparency and accountability that a military engagement would have. So an operation can amount to roughly eight times the scale of the opening round of the Kosovo war, and yet no one conceives of it as a 'war'. Now, let me be clear: I actually agree with the goal of many of these operations. But I am concerned about the technology's impact on how we talk about it and thus conceptualize and authorize it.

But we are also now seeing this trend – and I think this is a real game-changer – having an impact also on *overt* military operations. The Libya campaign is a great illustration of that. The authorization for the overt use of force by the US military was shaped by the War Powers resolution, which recognizes that sometimes there are emergencies and that the President needs to be able to deploy forces. But the resolution says that, within 60 days, Congressional approval must be obtained. This resolution is a post-Vietnam law, developed to ensure no more incidents like

the Gulf of Tonkin. But, when it got to the 60-day mark, the response from the Executive Branch was: 'We do not need authorization because it no longer involves risk to American servicemen or the threat thereof.' Essentially, the argument was that because people were no longer going into harm's way, the rules of that law no longer needed to be followed.

Yet we were still doing something that we used to think of as war. We were still blowing up things and people. That is, by that point, the operation had shifted to using unmanned systems, and after that 60-day mark, 146 air strikes using Predator/Reaper class systems were conducted, including the very last one that got Gaddafi. Now, again, let me be clear: I actually agreed with that operation; I had no sympathy for Gaddafi. But my concern is that we wanted to do something that we traditionally would have called a war, and yet the manner in which the various branches of government and the estates beyond them – the media, the public – thought about it was fundamentally different. We are setting enormous precedents without reflection on where they take us in the future.

In other words, we are saying that we do not have to go through the old ways of authorizing actions, because we now have this new technology. This changes the way we think of war. In a democracy, we used to think of war both as people going into harm's way and as bad things happening on the battleground. Now, technology has allowed us to disentangle the two, or at least led us to think that we can disentangle the two. This changes how we deliberate on war.

This does not just apply to unmanned systems and robotics. It also carries over to many other new technologies. Cyber is a good illustration of this. Militaries are able to engage in acts that might have previously been interpreted as war, but do not consider those acts as acts of war, either because they do not involve people in harm's way, or they are so fast moving – or actually so slow moving, to include some kinds of digital sabotage – that they do not fit the traditional understanding of war.

Does your statement also apply to the way non-state armed actors engage in war today? On the one hand, one could say that today not many non-state armed actors have sufficient resources to deploy drones and launch over 300 attacks over the course of several months. On the other hand, one could also say that the proliferation of new technologies is 'democratizing' warfare by making weaponry available to everyone. What do you see as emerging trends for the future?

First, we are definitely seeing a lowering of the barriers to war, not just for states, but for a wider variety of actors. This is not just with the most sophisticated technology. The AK-47 is a good illustration of that – a relatively simple technology could be a big advancement in that a child soldier using an AK-47 suddenly had the firepower of a Napoleon-era regiment. He may not be as professional, but he can create as much chaos, death, and destruction around him, all because of an AK-47 that he could learn how to use within thirty minutes. So the 'democratization' of war is not necessarily dependent only on the availability of high-end technology, but simply on technology that everyone can access.

Second, today we are definitely seeing a wide range of actors with access to new advanced technology, particularly as it becomes cheaper and simpler to use. On the non-state actors' side, just for robotics, the users already range from militants and quasi-terrorist groups to criminal groups, quasi-vigilante groups also known as border militias, media organizations, and even real estate agents. They have all started to use robotics, and when the point is reached where a microdrone can be flown using an iPhone application – which is possible now – then suddenly a lot of people can use it.

The same applies to computer technologies and cyber capabilities. However, we must not overstate the risks and fears, which is something that has really hit the cyber side with the accompanying hype to discussions of cyber terrorism. We have not yet seen the first successful cases of grand terrorism using cyber means, or successful cases of grand military operations. One reason for that – particularly on the terrorism side – is that the conduct of an effective cyber operation, to use the example of Stuxnet, does not just involve having expertise in cyber; it involves having a fairly significant and capable intelligence effort, combined with expertise in a number of different areas.

Take the example of Stuxnet. It was not just about cracking into an Iranian computer network, but it was also about specifically designing a fairly sophisticated piece of malware, targeting specific Siemens-made systems operating in that specific nuclear facility. The questions of how these systems operate, how many of them there are, and how to best crack them are only answered by a combination of intelligence and engineering expertise. A lot of different expertise came together. This is neither something that a couple of 14-year olds sipping Red Bull can do, nor is it something that a couple of would-be terrorists hiding out in an apartment in Hamburg will be able to figure out.

So, I am afraid that sometimes hysteria and hype can drive us in areas that maybe do not deserve our utmost attention, be it in policy circles or among humanitarian practitioners.

Let us continue our discussion on lowering the costs of war down to the ground. If one looks at the US in terms of the global projection of force, the US can decide to take action if another country is 'unable or unwilling' to act against a threat to the US. The use of drone strikes in Pakistan, Yemen, and Somalia has been explained with this reasoning. What if another country were to say that the US is 'unable or unwilling'?

A real challenge facing the humanitarian community when in talking about these 'drone strikes' is the conflation the tactics and the technology. Let us use the case of the US strike in Yemen that got Al Awlaki – a particularly heated case because it involved a US citizen. Was it the fact that it was a drone that carried out the strike that upset the humanitarian community, or was it the strike itself? That is, when we complain about 'drone strikes', what if we had used a manned F-16 rather than MQ9 Reaper? Are you now okay with it? Of course not. Technology shapes the politics around it and the decisions that are made, but some of the legal questions do

not turn on that technology itself. It will usually be the action itself and how we weigh it that determines whether an act is legal or not.

Similarly, there can be a conflation between the use of the technology in declared war zones and the use of technology outside declared war zones. For example, we are sometimes asked about the US military use of these systems, but questioner will really be asking about 'drone strikes' in Pakistan. The US military use of systems is not that problematic from a humanitarian law perspective. It takes place within war zones, within a fairly transparent chain of command. There is a system of accountability that reacts when things go wrong, there are reporting mechanisms, and a legal system that can deal with it.

More importantly, the targeting questions are a lot easier in a transparent war zone. For me, the big key is that action, rather than identity, is the driving force. One does not have to know someone's name for them to be a viable target in a war zone. If a sniper shooting at you, whether you think it is Albert or Ahmed behind the gun, it does not matter – the act of them shooting does. But when you cross the border to, say, Pakistan, and the engagement is moved out of a military system and support of troops on the ground that involves a clear chain of command, the military justice system, and the operation being run out of a civilian intelligence process, and where the targeting is based not on action, but more on perceived identity and likely threat, that is when it gets problematic.

So, the different rules under which you operate, in everything from your authorization of the actions to the legal consequences for mistakes (or, frankly no legal consequences as in the actual practice), are fundamentally different when the operation using robotics drones moves from being a military one in a warzone to a covert one across the border. Now some will say this is not the way it should be, but of course that is the difference between 'should' and 'is'.

Can new technologies benefit the humanitarian community?

For the humanitarian world, just as for the military, there are parallel potentials and problems arising from new technologies. Technology is giving humanitarians capabilities that they did not imagine they would have a generation ago, but is also creating questions for the humanitarian community that it did not imagine it would be addressing a generation ago; for instance, capabilities to detect and document war crimes in a way that was never dreamed of. The ability today for someone to get away with the world not knowing that they are committing genocide is very slim.

Similarly, big and small organizations alike have the ability to document, respond to natural disasters, and find where people are when they need help. Compare the responses to the 2004 tsunami and to the 2010 earthquake in Haiti – just a couple of years after the tsunami, humanitarian organizations were able to share information on where people were, and what kind of help they needed, using Twitter, crisis maps, and drones. These capabilities are amazing.

At the same time, deep questions that we did not have before arise: what kind of capability should a non-governmental humanitarian actor have? Should it have its own air force-like equivalent? Under what rules and regulations does it

operate? Issues of privacy, of ownership and management of information, etc., also need to be addressed. And, most importantly, in some instances there are false hopes involved, again parallel to the military vision that some have of robotics as a silver-bullet technological solution. Some, for instance, argue that having drones deployed to Sudan or Syria to monitor war crimes there would stop them. But we already know that there are bad things happening in Darfur and Damascus. Now there is a slightly better picture of those things. It might help create more Twitter posts, but does it actually mean the reality on the ground is altered?

Essentially, think of it this way: Henry Dunant did not imagine a world in which the ICRC would be weighing its thoughts on flying machines that had no people inside them, that crossed borders to drop rockets that fired with precision such that they always hit where there is a light amplified beam. The organization during his time was not even ready to wrestle with things such as undersea boats. So the questions that the organization will be weighing in on today and in the future are very different.

What kind of humanitarian consequences can arise from these new technologies?

A big challenge in how we talk about the humanitarian consequences is disentangling the technology of today from the technology that is looming.

For instance, some people claim that drones cannot take prisoners. Well, during the 1991 Gulf War, there was a Pioneer drone used by the US Navy for targeting for naval gunfire. The Iraqis figured out that every time this loud little propeller plane flew above them, in a couple of minutes all hell would break loose. The drone was scouting for a Second World War era battleship that fired 16-inch cannon shells that level everything within the radius of a football field. So the Iraqis worked out that this little drone was bad news when it came near them, and so a a group of them, the next time it flew over, took off their uniforms and waved white T-shirts. It's the first case in history of people surrendering to a robot.

My point is that this episode happened in 1991. Remote technology, such as the Pioneer and much of robotics, still today has a man in the loop. And yet they already have massive consequences, even though they are the first generation of this technology. We do not have to wait for fully autonomous technology in some imaginary 'Terminator world' for robotics to have an impact on when and where we go to war. It is already happening now in Pakistan and Libya. But often, we either conflate or ignore even more important questions as the technology gains more and more autonomy and intelligence. Currently, the questions revolve around the use of drones in non-war zones, and around the element of remoteness of such strikes, and how that affects civilian casualties.

However, we are moving into the debate on systems that make increasingly autonomous decisions; the point of human interface with such machines is not in the midst of battle, but rather in the days, weeks, or even years prior to it when someone programmes the system. For instance, we already have target-acquisition software, and we already have planes that not only can take off and land on their

own, but can fly for certain parts of the mission on their own. In the future, there may be an autonomous system that can turn a 50-calibre machine gun into, in effect, a sniper rifle.

Our current artificial intelligence, though, cannot effectively distinguish between an apple and a tomato. Any two-year-old boy can distinguish between them. Let us also look at emotional intelligence. A computer looks at an 80-year-old woman in a wheelchair the exact same way it looks at a T-80 tank. They are both just zeros and ones. So there are parts of the human experience of war that may be shifted or changed or moved as technology that is increasingly more capable evolves.

And again, just as it was for me when I went around to humanitarian organizations interviewing them for my book four years ago, and none of them were ready or willing to talk about technologies like the Predator, the same phenomenon is playing out right now with the current development of technology. The humanitarian community is *ex post* reacting to things that already exist and are being used. And thus its impact will be less because of that, because the community did not weigh in until it was already behind the curve. The next technology is already coming along.

And it is hard blame them – there is really so much else going on in the world that it would seem like a waste of time to think about robotics. Then again, the technology we talk about today is not at all theoretical: it is not being developed in some secret desert labs that no one knows about. It exists, and we can read about it in *Wired* magazine[5] or watch it on the news, and yet we are behind it. Certainly, there is classified work in various areas, but so much of the work is out in the open. I am working on a project right now in which the goal is to identify the looming game-changing technologies, in other words, what are the technologies that are where the Predator was in 1995. And let us not forget that the Predator was openly flown in 1995. It was not secret.

What can international civil society – and the humanitarian community in particular – do to better respond to the challenges you mention? How can we be one step ahead?

I wrote an article called 'The ethics of killer apps: why is it so hard to talk about science, ethics and war'.[6] In it, I work through a series of challenges that we face today when we talk about new technology, and one of the biggest challenges I identified is that we do not integrate well across fields. We stay within our own field of expertise, surrounded by people who think like us, use our language, and write and read journals only in our field, and we reward each other on that basis.

The result is that crossing these fields is a lot like crossing, literally, national cultural borders. If you speak the language of humanitarian law, and you go into the

5 Available at: http://www.wired.com/magazine/ (last visited June 2012).

6 Peter W. Singer, 'The ethics of killer apps: why is it so hard to talk about science, ethics and war', in *Journal of Military Ethics*, Vol. 9, No. 4, 2010, pp. 299–312.

world of science, it is as if everybody is speaking Finnish. In turn, when the scientist tries to read, write, or talk to someone in the humanitarian law field, it is as if everybody is speaking Portuguese to them. And it is not just the languages that are different – there is a fundamental inability to understand. The bottom line of this is that – as one of my interviewees put it – a scientist would rarely engage in a philosophical discussion on the development of new technologies because that would require him to 'wear the hat of a philosopher', and he 'does not own that hat'. In turn, one can now read tonnes of articles in the international law community on issues such as drones that are written by someone who has never seen a drone, nor never even tried to talk to someone who has flown them, designed them, or operated them. So we have these disconnects, which I think are the biggest problem.

For the project that I mentioned earlier, we are actually going out and interviewing top scientists, military lab directors, futurologists, people who work at places like Google and the like, and basically asking them the question: what are the new technologies that will shape the future? Are these technologies going to be like the AK-47, that everybody will have, or like the atomic bomb, which very few actors can acquire? The next question is how will the military use these weapons. What are the uses in high-end, state-oriented conflicts, and what are the uses in non-state, low-end insurgency type of conflicts? How might someone use these technologies against you, and what are the vulnerabilities of these technologies? The final part of this project is gathering the ethicists, the philosophers, the humanitarian lawyers, the religious leaders, and the media and saying: here are the technologies the scientists think are coming; here are the ways the military's thinking about using them; what is your take on this? The idea is to try, at an earlier stage, to ask the questions that we know are looming. That, to me, is the best way to go about it, rather than waiting until after the fact to engage in the discussion. Prepare yourself.

Another part of the challenge for the humanitarian community is, much like any other field, we focus only on a certain part of the big questions we want to tackle and are often not judicious in our efforts. For instance, during my research on child soldiers I found that an oddly large percentage of the discourse around child soldiers focused on the practice of Western militaries of recruiting of 17-and-a-half-year olds, something that involved a couple of hundred people who were not abducted from their homes. One would read the reports, which would cover this problem with at least the same depth and focus and energy as the problem of tens of thousands of children 12-years-and-under being abducted from their homes, shot up with brown-brown, and forced to burn down a village. Both were wrong practices, in my mind, but obviously the second is worse and should receive more of our limited resources. If we are to have effect and to spin-up energy around an issue, we have to know clearly where we really want to put our efforts.

Today, we can see this with weapons and technology discussions. Blinding lasers were the target of much discourse at a point in time when their impact did not match the extent of the discourse. Again, let me be clear, I am not saying these efforts are not worthy, but they need to be made with an awareness of how the international humanitarian community can best use its resources, and where the maximum impact will be.

I fear that we sometimes trend towards issues that either sound sexy or are more likely to draw media attention (and, thus, donor attention), but they might not have the same impact as other less well-publicized issues. For instance, in the 1990s there was a higher per capita percentage of humanitarian workers in the Balkans than there was in places in Africa where there was as much – or more – trouble. Today we see the same phenomenon in technology activism, and that concerns me.

In your research, do you see a differentiation in terms of the ethical approach to uses of technology? Do the ethical processes that would need to be considered before we deploy new technologies differ in different contexts around the world (e.g. China, Russia, India)?

Absolutely, because people are shaped by their psychology and their culture this is another big impact on what we think is the right or wrong of these technologies. A good example of this is attitudes towards robotics. In the West, the robot, from the very start, has always been the mechanical servant that wised up and then 'rised up'. Literally, the word is taken from the Czech word for 'servitude', and first used in a 1920s play called *R.U.R: Rossum's Universal Robots* in which these new mechanical servants, called 'robota', become smart and take over the world. That narrative of the robot as evil and ready to take over has continued today throughout our science fiction, but also in our policy world. You know, a picture of a machine-gun-armed robot, even if it is a completely remotely operated system, is still something spooky to us.

In Asia, by comparison, the robot – in science fiction and beyond – has been looked at differently. In Japan, for example, after the end of the Second World War the robot emerged in their sci-fi and was not the bad guy, but rather almost always the good guy. The robot is the humanitarian actor. *Astro Boy* is an example. There are parallel certain notions in religion and culture. In Shintoism, for example, unlike in the West, a rock has a soul, a stream has a soul, and a robot has a soul. The result is that we see very different attitudes towards robotics in different cultures, and different comfort levels about using them in the home. We do not have babysitter robots in the West today. We do not see marketization of elderly companion robots. But they have them in Japan. In South Korea, Samsung not only made a machine-gun-armed robot, but actually created a TV commercial around how cool it was that they had built a machine-gun-armed robot. Can you imagine Apple celebrating itself in the West with a TV commercial advertising that they have created a machine-gun-armed robot?

Are robots actually able to behave ethically? Can robots improve the respect for the law of war in the field, or do you see their deployment as a threat?

We want an easy yes or no answer, or in robotic terms, a zero or one framing of the issues. And yet I think that actually illustrates exactly why we will not see the ethical

problems solved by robotics. At the end of the day, neither war nor ethics is a realm of just zeros and ones, even with the most sophisticated robotics.

We are already seeing capability enhancements that will allow us to observe or respect international law or, even more importantly, catch people violating it, in a way that we could not previously imagine. I will use a US military example, told to me by an officer in Iraq. They had an unmanned aerial system flying overhead while they were conducting a ground operation. They captured an insurgent and he was in an alley way, and a soldier was guarding him; the soldier looked one way down the street, looked the other way, saw no one watching, and gave the detainee a good swift boot to the head. But he did not factor in the drone. Everyone in the command centre was watching via the plane overhead. And the commander talked about how everyone in the command centre then turned and looked at him, wondering what he was going to do about it. Previously, documentation of this case of prisoner abuse would have been impossible, and instead now everyone sees it and looks at the commander for the 'what next'? He punished the guy.

Another scenario that illustrates the advantage of these technologies is robots that can substitute for soldiers in urban settings. Soldiers in these operations have to burst into a room, and within literally milliseconds decide whether the people inside are civilians or enemies. Is that man is holding an AK-47 or a camera, or is that child really holding rifle or a broom? They know that if they get it wrong in those milliseconds, they might die. So a lot of mistakes happen. Compare this with sending robots in instead: they can detect the people, look at them, and they get it wrong, they can wait to shoot. If the people shoot first, so what? No one dies. This is the strong potential advantage of these technologies.

But let me be very clear, many people take these notions too far and argue that technology will be the silver-bullet ethical solution. Our souls are not perfect, neither are our machines. So we should not talk about technology that does not yet exist as if it is real. So it is said, we could put an 'ethical governor' on technology and it would solve the problems. Ask to see the design of the ethical governor. It is what we call, on the military side, vapourware. There is hardware, software, and vapourware. It literally does not exist.

But even if it did exist, it is still not a silver bullet. Let us imagine that we could create a software package that would implement the Geneva Conventions. The reality is that this still would not be enough in modern war. We've still got two problems. First, the fact that the Geneva Conventions do not turn into an easy language of yes or no in all situations, particularly in modern conflict. Second, we have actors that are engaging in what we call 'lawfare', who know the laws of war, and deliberately violate the laws of war.

So I use these real world examples to illustrate the problem of thinking that technology will solve wars and the dilemmas of war. Even assuming the technology is created, what would it tell you to do when you have a sniper shooting at you with two women sitting in front of him and four kids lying on top of him as a real world sniper did in Somalia? A sniper who had given himself a living suit of non-combatant armour. Shoot or not shoot? What would it tell you when it saw a tank conducting ethnic cleansing with kids riding on top of it? What would it tell you to

do with an ambulance that moves both wounded soldiers and civilians, and munitions? What would it tell you to do to a civilian who is being blackmailed into firing rockets from his farm? He is firing the rockets into a civilian city, but if he does not he will be killed by the local militant group. These are all real world cases from recent conflicts. We could spend hours and hours arguing about it – the pages of this journal would be filled with articles about what the law does and does not say, and all the lawyers would have a great time arguing about what to do in those types situations. So to think the dilemmas of conflict are somehow easily resolvable by a software package that does not yet exist is not sound.

And, of course, in war the enemy has a vote. That is, as there are more and more advanced machines, people will become more and more advanced in figuring ways around them. I give this anecdote – it's a great one. There is an unmanned ground vehicle that mounts a machine gun. I was speaking with a group of US Marines about it, not just the incredible advanced nature of it, but also the other side's potential reactions. And we talked about the fact that the most effective counter against it was not some super-secret counter-technology. Rather, it was a six year old armed with a can of spray paint, because that child creates an incredible dilemma.

You either shoot a six year old, who is technically unarmed, because he has a can of spray paint, or you allow a six year old to walk up to your system and defeat it. He just sprays the visual sensors. One of the marines in the audience yelled out: 'Well, we'll just upload a non-lethal weapon, and taser that little guy. I said, 'Well, that's interesting, that is actually a pretty humanitarian answer.' Except there is still a problem. You have given a humanitarian response; you have come up with a solution around it. But you still actually have multiple problems.

The first problem is: what is the likely cost of the upgrade package? One of the Marines, half jokingly, commented that with our acquisition system, it would likely cost a couple of million. Okay, so you are now fighting an investment war between a 50-cent can of spray point and you are responding with multimillion-dollar upgrades. That is unsustainable. The other side has immediately won simply because of using that unlawful tactic, by sending a kid out to fight for them. Second, even if you take this 'non-lethal' route it is still going to be bad news. When the video goes viral, of a robot tasering a six year old, I think it is still going to be bad press, and will still reverberate. My point is this: you can have very advanced technology, but you cannot get rid of the ethical and legal dilemmas that encompass battlefield tactics and strategies.

We seem to be somehow fascinated with robots – military and humanitarian actors alike. Where will this fascination take us in the future?

Well, you can answer this with the meta-challenge and then the meta-question. The meta-challenge is essentially this: technology is advancing at an exponential pace. In the IT world, it is following, effectively, Moore's Law: it is doubling itself every 18 months. The non-military example of this would be the iPhone that you gave your kid that seemed so incredibly advanced and powerful last year is outdated this year.

We see the battlefield version of that: the entire US Army that my father served in had less computing power at its disposal than is encompassed within a single greeting card that opens up and plays a little song. And yet our political policy and legal and ethical communities do not move at an exponential pace; they move at a fairly glacial pace. So the disconnect between the two is getting greater and greater; we are falling further and further behind. So this is the meta-challenge.

The meta-question that robotics provoke is this: we distinguish ourselves as a species because of our creativity; we are the only species that created fire, that created rockets that took us to the moon, that created art, that created literature, that created laws and ethics. That is what distinguishes us as a species. And now we are creating not just incredible machine technology, but a potential new species, maybe in our image, maybe not. But if we are honest with ourselves, the reason that we are creating this technology is not just about advancement in a positive way, it is that age-old human story of trying to figure out how to kill one another better. So the title of my book, *Wired for War*, was a play on words. The bottom-line question is: is it our machines that are wired for war, or is it us humans that are actually the ones wired for war?

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

New capabilities in warfare: an overview of contemporary technological developments and the associated legal and engineering issues in Article 36 weapons reviews

Alan Backstrom and Ian Henderson*

Alan Backstrom, BEng, MEngSci, is an automotive engineering quality manager. He has extensive experience working with original equipment manufactures, system suppliers, subsystem suppliers, and component suppliers, with a particular focus on major design validation techniques, warranty analysis, and accident investigation.

Group Captain Ian Henderson, AM, BSc, LLB, LLM, PhD, is a legal officer with the Royal Australian Air Force.

Abstract

The increasing complexity of weapon systems requires an interdisciplinary approach to the conduct of weapon reviews. Developers need to be aware of international humanitarian law principles that apply to the employment of weapons. Lawyers need to be aware of how a weapon will be operationally employed and use this knowledge

* This paper was written in a personal capacity and does not necessarily represent the views of the Australian Department of Defence or the Australian Defence Force. Thank you to many friends and colleagues who generously provided comments on the draft.

doi:10.1017/S1816383112000707

to help formulate meaningful operational guidelines in light of any technological issues identified in relation to international humanitarian law. As the details of a weapon's capability are often highly classified and compartmentalized, lawyers, engineers, and operators need to work cooperatively and imaginatively to overcome security classification and compartmental access limitations.

Keywords: weapon, international humanitarian law, law of armed conflict, warfare, IHL, LOAC, Geneva, additional protocol, weapons review, autonomous, target recognition, reliability.

Article 36 of Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts provides:

> In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.[1]

As weapons become more technologically complex, the challenges of complying with this apparently simple requirement of international law become more daunting. If a lawyer were to conduct a legal review of a sword, there would be little need for the lawyer to be concerned with the design characteristics beyond those that can be observed by the naked eye. The intricacies of the production and testing methods would equally be legally uninteresting, and even a lawyer could grasp the method of employment in combat. The same cannot be said about some modern weapons, let alone those under development. The use of a guided weapon with an autonomous firing option requires an understanding of the legal parameters; the engineering design, production, and testing (or validation) methods; and the way in which the weapon might be employed on the battlefield.[2] While somewhat tongue-in-cheek, there is some truth to the view that a person becomes a lawyer due to not understanding maths, another becomes an engineer due to not understanding English, and the third a soldier due to not understanding either!

1 Opened for signature 12 December 1977, 1125 UNTS 3, entered into force 7 December 1978 (API). See generally Justin McClelland, 'The review of weapons in accordance with Article 36 of Additional Protocol I', in *International Review of the Red Cross*, Vol. 85, No. 850, June 2003, pp. 397–415; Kathleen Lawand, 'Reviewing the legality of new weapons, means and methods of warfare', in *International Review of the Red Cross*, Vol. 88, No. 864, December 2006, pp. 925–930; International Committee of the Red Cross (ICRC), *A Guide to the Legal Review of New, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*, 2006. For a thorough discussion of what is and is not a 'weapon' for the purposes of legal review, see Duncan Blake and Joseph Imburgia, '"Bloodless weapons"? The need to conduct legal reviews of certain capabilities and the implications of defining them as "weapons"', in *The Air Force Law Review*, Vol. 66, 2010, p. 157.

2 See Michael Schmitt, 'War, technology and the law of armed conflict', in Anthony Helm (ed.), *The Law of War in the 21st Century: Weaponry and the Use of Force,* Vol. 82*, International Law Studies*, 2006, p. 142.

Our purpose in writing this article is to breakdown those barriers through a multidisciplinary approach that identifies the key legal issues associated with employing weapons, setting out important features of emerging weapons, and then analysing how engineering tests and evaluations can be used to inform the weapon review process. Through the combination of the above methods, we hope to provide a general framework by which the legal and engineering issues associated with weapon development and employment can be understood, regardless of the simplicity or complexity of the weapon.

We commence with a brief review of the key legal factors for employing and reviewing weapons, followed by three substantive parts. The first part deals with the target authorization process, regardless of the choice of weapon to be employed. The second part looks at some emerging weapons and the legal issues associated with those weapons. The final part considers the engineering issues associated with weapon reviews and, in particular, how an understanding of engineering processes can assist when reviewing highly complex weapons.

Key legal factors

The key legal steps under international humanitarian law[3] when conducting an attack can be summarized as:

1. collecting information about the target;
2. analysing that information to determine whether the target is a lawful target for attack at the time of the attack;
3. appreciating the potential incidental effects of the weapon and taking feasible precautions to minimize those effects;
4. assessing the 'proportionality' of any expected incidental effects against the anticipated military advantage of the overall attack (not just the particular attack of the individual weapon);[4]
5. firing, releasing, or otherwise using the weapon such that its effects are directed against the desired target;
6. monitoring the situation and cancelling or suspending the attack if the incidental effects are disproportionate.[5]

In addition, consideration must also be given to the type of weapon to be employed, and particularly relevant to this article is that there are also ways of employing (using) an otherwise lawful weapon that might result in a banned effect (e.g., indiscriminately firing a rifle). The key legal factors when conducting the review

3 Also known as the law of armed conflict.

4 See, for example, Australia's declaration of understanding to the effect that military advantage in Articles 51 and 57 of API, above note 1, means 'the advantage anticipated from the attack considered as a whole and not from isolated or particular parts of the attack' – reprinted in Adam Roberts and Richard Guelff, *Documents on the Laws of War*, 3rd edn, Oxford University Press, Oxford, 2000, p. 500.

5 See above note 1, Article 57(2)(b) of API.

of new weapons (including means and methods of combat) are whether the weapon itself is banned or restricted by international law;[6] and if not, whether the effects of the weapon are banned or restricted by international law.[7] Finally, the 'principles of humanity and the dictates of the public conscience' must also be kept in mind.[8]

From an operational point of view, the key points can be expressed as: achieving correct target-recognition, determining how to exercise weapon release authorization, and controlling (or limiting) the weapon effect.

With weapons of relatively simple design, the associated legal issues are simple. With the sword example above, the only real issues are whether it is a 'banned weapon';[9] and if not, whether the person who wields it does so with discrimination. Any design flaws (e.g., poorly weighted) or manufacturing defects (e.g., metal is too brittle) are unlikely to affect the legal analysis and are primarily the worry of the person using the sword. With more complex weapons like crossbows, the complexity of the weapon design introduces the potential for discrimination to be affected by:

- design errors (e.g., the weapon does not fire straight or consistent with any sighting mechanism as the design is flawed); or
- manufacturing errors (e.g., the weapon does not fire straight or consistent with any sighting mechanism as the weapon was not built, within tolerance, to the design).

These types of errors have the potential to be magnified with long-range weapons (such as artillery) and batch variation now also becomes a significant factor as any variations are magnified over the longer range of the weapon. Further, modern

6 Weapons can be banned outright, banned based on designed purpose or expected normal use, or the means of employment can be regulated (i.e., banned uses). A weapon may be totally banned through specific law (e.g., biological weapons are prohibited under the *Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction*, opened for signature 10 April 1972, 1015 UNTS 163, entered into force 26 March 1975), or may be banned generally if in all circumstances it is a weapon that is 'of a nature to cause superfluous injury or unnecessary suffering', see above note 1, Article 35(2) of API, and associated customary international law. Contrast this with, for example, laser weapons, which are generally lawful but are prohibited when they are specifically designed, solely or as one of their combat functions, to cause permanent blindness to unenhanced vision (*Protocol (IV) on Blinding Laser Weapons to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects*, opened for signature 13 October 1995, 35 ILM 1218, entered into force 30 July 1998). Finally, incendiary weapons are per se lawful, but, for example, may not be employed by air delivery against military objectives located within a concentration of civilians, see Article 2(2) of *Protocol III on Prohibitions or Restrictions on the Use of Incendiary Weapons to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects*, opened for signature 10 April 1981, 1342 UNTS 137, entered into force 2 December 1983.

7 ICRC, *A Guide to the Legal Review of New, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*, above note 1, p. 11.

8 *Ibid.*

9 As there is no specific ban on swords, the issue would be a review under the general prohibition on weapons that cause unnecessary suffering pursuant to Article 35(2) of API, above note 1.

weapons have a variety of aiming mechanisms that are not solely dependent on the operator, such as inertial guidance, global positioning system (GPS), and electro-optical guidance. Finally, as discussed below, there is even the capacity for the weapon itself to select a target.

Weapon technology is advancing in many different areas and there is limited public material available on the avenues of research and the capabilities of the weapons being developed.[10] The following emerging weapons are, therefore, purely representative. In any event, the exact capabilities are of less importance to the discussion than are the general modes of operation.

Target recognition and weapon release authorization

The following discussion deals with weapons and weapon systems that have some level of functionality to discriminate between targets and, in appropriate circumstances, might attack a target without further human input. For example, a non-command-detonated landmine is a weapon that once placed and armed, explodes when it is triggered by a pressure plate, trip wire, etcetera. Such landmines have a very basic level of target recognition (e.g., a pressure plate landmine is triggered when a plate is stepped upon with a certain minimum amount of weight – e.g., 15 kilograms – and is clearly unlikely to be triggered by a mouse) and require no human weapon-release authorization.[11] More complex weapon systems purport to distinguish between civilian trucks and military vehicles such as tanks.[12] Automated and autonomous weapon systems need to be distinguished from remotely operated weapon systems. While there has been much discussion lately of unmanned combat systems, these are just remotely operated weapon platforms and the legal issues depend far more on the manner in which they are used than on anything inherent to the technology.[13] The following discussion differentiates automated weapons from autonomous weapons, briefly reviews some key legal issues associated with each type of weapon system, and concludes by outlining some methods for the lawful employment of such weapon systems.

10 See Hitoshi Nasu and Thomas Faunce, 'Nanotechnology and the international law of weaponry: towards international regulation of nano-weapons', in *Journal of Law, Information and Science*, Vol. 20, 2010, pp. 23–24.

11 Of course, this can be the very problem with landmines. Non-command-detonated landmines placed in areas frequented by civilians cannot distinguish between a civilian and a combatant activating the trigger mechanism.

12 'Anti-vehicle mines, victim-activation and automated weapons', 2012, available at: http://www.article36.org/weapons/landmines/anti-vehicle-mines-victim-activation-and-automated-weapons/ (last visited 1 June 2012).

13 For discussions of how such remotely operated systems are, legally, just like any other weapon system and are not deserving of separate categorization or treatment under international humanitarian law, see generally *Denver Journal of International Law and Policy*, Vol. 39 , No. 4, 2011; Michael Schmitt, Louise Arimatsu and Tim McCormack (eds), *Yearbook of International Humanitarian Law 2010*, Springer, Vol. 13, 2011.

Automated weapons

Automated weapon systems:[14]

> are not remotely controlled but function in a self-contained and independent manner once deployed. Examples of such systems include automated sentry guns, sensor-fused munitions and certain anti-vehicle landmines. Although deployed by humans, such systems will independently verify or detect a particular type of target object and then fire or detonate. An automated sentry gun, for instance, may fire, or not, following voice verification of a potential intruder based on a password.[15]

In short, automated weapons are designed to fire automatically at a target when predetermined parameters are detected. Automated weapons serve three different purposes. Weapons such as mines allow a military to provide area denial without having forces physically present. Automated sentry guns free up combat capability and can perform what would be tedious work for long hours and without the risk of falling asleep.[16] Sensor-fused weapons enable a 'shot and scoot' option and can be thought of as an extension of beyond-visual-range weapons.[17]

The principal legal issue with automated weapons is their ability to discriminate between lawful targets and civilians and civilian objects.[18] The second main concern is how to deal with expected incidental injury to civilians and damage to civilian objects.[19]

Starting with the issue of discrimination, it is worth noting that automated weapons are not new. Mines, booby traps, and even something as simple as a stake at the bottom of a pit are all examples of weapons that, once in place, do not require further control or 'firing' by a person. Some of these weapons also have an element of discrimination in the way they are designed. Anti-vehicle mines, for example, are

14 Not to be confused with automatic weapons, which are weapons that fire multiple times upon activation of the trigger mechanism – e.g., a machine gun that continues firing for as long as the trigger remains activated by the person firing the weapon.

15 Jakob Kellenberger, ICRC President, 'International humanitarian law and new weapon technologies', 34th Round Table on Current Issues of International Humanitarian Law, San Remo, 8–10 September 2011, Keynote address, p. 5, available at: http://iihl.org/iihl/Documents/JKBSan%20Remo%20Speech.pdf (last visited 8 May 2012). Various types of existing automated and autonomous weapons are briefly discussed, with further useful citations, in Chris Taylor, 'Future Air Force unmanned combat aerial vehicle capabilities and law of armed conflict restrictions on their potential use', Australian Command and Staff College, 2011, p. 6 (copy on file with authors).

16 South Korea is developing robots with heat and motion detectors to sense possible threats. Upon detection, an alert is sent to a command centre where the robots audio or video communications system can be used to determine if the target is a threat. If so, the operator can order the robot to fire its gun or 40 mm automatic grenade launcher. 'S. Korea deploys sentry robot along N. Korea border', in *Agence France-Presse*, 13 July 2010, available at: http://www.defensenews.com/article/20100713/DEFSECT02/7130302/S-Korea-Deploys-Sentry-Robot-Along-N-Korea-Border (last visited 6 May 2012).

17 A sensor-fused weapon is a weapon where the arming mechanism (the fuse) is integrated with a target detection system (the sensor).

18 Issues such as fratricide are not, strictly speaking, a concern of international humanitarian law. In any event, other means and methods are adopted to reduce fratricide, such as 'blue-force trackers', safe corridors, and restricted fire zones.

19 See above note 1, Article 51(5)(b) and Article 57(2)(a)(iii) of API.

designed to explode only when triggered by a certain weight. Naval mines were initially contact mines, and then advanced to include magnetic mines and acoustic mines. Of course, the problem with such mines is that there is no further discrimination between military objectives or civilian objects that otherwise meet the criteria for the mine to explode.[20] One way to overcome this is to combine various trigger mechanisms (sensors) and tailor the combination towards ships that are more likely to be warships or other legitimate targets than to be civilian shipping.

As weapons have become more capable and can be fired over a longer range, the ability to undertake combat identification of the enemy at greater distances has become more important. Non-cooperative target recognition (also called automatic target recognition) is the ability to use technology to identify distinguishing features of enemy equipment without having to visually observe that equipment.[21] A combination of technology like radar, lasers, communication developments, and beyond-visual-range weapon technology allows an ever-increasing ability to identify whether a detected object is friendly, unknown, or enemy and to engage that target. With each advance though, there is not 'a single problem but rather . . . a continuum of problems of increasing complexity ranging from recognition of a single target type against benign clutter to classification of multiple target types within complex clutter scenes such as ground targets in the urban environment'.[22] Significant work is underway to produce integrated systems where cross-cueing of intelligence, surveillance, and reconnaissance sensors allows for improved detection rates, increased resolution, and ultimately better discrimination.[23] Multi-sensor integration can achieve up to 10 times better identification and up to 100 times better geolocation accuracy compared with single sensors.[24]

With something as simple as a traditional pressure-detonated landmine, the initiating mechanism is purely mechanical. If a weight equal to or greater than the set weight is applied, the triggering mechanism will be activated and the mine will explode. This type of detonation mechanism cannot, by itself, discriminate between civilians and combatants (or other lawful targets). The potential for incidental injury at the moment of detonation is also not part of the 'detonate/do-not-detonate' equation. While this equation can be considered with

20 Except where the mine is command-detonated.

21 One example is using laser beams (an alternative is millimetre wave radar) to scan an object and then use processing algorithms to compare the image to pre-loaded 3D target patterns. Target identification can be based on specific features with up to 15cm resolution at a distance of 1000 metres. See 'Lased radar (LADAR) guidance system', Defense Update, 2006, available at: http://defense-update.com/products/l/ladar.htm (last visited 8 May 2012).

22 'RADAR Automatic Target Recognition (ATR) and Non-Cooperative Target Recognition (NCTR)', NATO, 2010, available at: http://www.rto.nato.int/ACTIVITY_META.asp?ACT=SET-172 (last visited 8 May 2012).

23 See Andy Myers, 'The legal and moral challenges facing the 21st century air commander', in *Air Power Review*, Vol. 10, No. 1, 2007, p. 81, available at: http://www.raf.mod.uk/rafcms/mediafiles/51981818_1143_EC82_2E416EDD90694246.pdf (last visited 8 May 2012).

24 Covering memorandum, *Report of the Joint Defense Science Board Intelligence Science Board Task Force on Integrating Sensor-Collected Intelligence*, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, US Department of Defense, November 2008, p. 1.

command-detonated landmines, that is clearly a qualitatively different detonation mechanism. With pressure-detonated landmines, the two main ways of limiting incidental damage are either by minimizing the blast and shrapnel, or by placing the mines in areas where civilians are not present or are warned of the presence of mines.[25]

However, the triggering mechanisms for mines have progressively become more complex. For example, anti-vehicle mines exist that are designed to distinguish between friendly vehicles and enemy vehicles based on a 'signature' catalogue. Mines that are designed to initiate against only military targets, and are deployed consistent with any design limitations, address the issue of discrimination. Nevertheless, that still leaves the potential for incidental injury and damage to civilians and civilian objects. The authors are not aware of any weapon that has sensors and/or algorithms designed to detect the presence of civilians or civilian objects in the vicinity of 'targets'. So, while some weapons claim to be able to distinguish a civilian object from a military objective and only 'fire' at military objectives, the weapon does not also look for the presence of civilian objects in the vicinity of the military objective before firing. Take the hypothetical example of a military vehicle travelling in close proximity to a civilian vehicle. While certain landmines might be able to distinguish between the two types of vehicles and only detonate when triggered by the military vehicle, the potential for incidental damage to the civilian vehicle is not a piece of data that is factored into the detonate/do-not-detonate algorithm. This is not legally fatal to the use of such automated weapons, but does restrict the manner in which they should be employed on the battlefield.

Along with discrimination there is the second issue of the potential for incidental injury to civilians and damage to civilian objects. The two main ways of managing this issue for automated weapons are controlling how they are used (e.g., in areas with a low likelihood of civilians or civilian objects) and/or retaining human overwatch. Both points are discussed further below under the heading 'Methods for the lawful employment of automated and autonomous weapons'. A third option is to increase the 'decision-making capability' of the weapon system, which leads us to autonomous weapons.

Autonomous weapons

Autonomous weapons are a sophisticated combination of sensors and software that 'can learn or adapt their functioning in response to changing circumstances'.[26] An autonomous weapon can loiter in an area of interest, search for targets, identify suitable targets, prosecute a target (i.e., attack the target), and report the point of

25 Of course, history has shown that many anti-personnel landmines were either emplaced without adequate consideration of, or worse intentional disregard for, the risk to civilians. As a result, a majority of states have agreed to a complete ban on the use of non-command-detonated anti-personnel landmines. See ICRC, 'Anti-personnel landmines', 2012, available at: http://www.icrc.org/eng/war-and-law/weapons/anti-personnel-landmines/ (last visited 8 May 2012).

26 J. Kellenberger, above note 15, p. 5.

weapon impact.[27] This type of weapon can also act as an intelligence, surveillance, and reconnaissance asset. An example of a potential autonomous weapon is the Wide Area Search Autonomous Attack Miniature Munition (WASAAMM). The WASAAMM:

> would be a miniature smart cruise missile with the ability to loiter over and search for a specific target, significantly enhancing time-critical targeting of moving or fleeting targets. When the target is acquired, WASAAMM can either attack or relay a signal to obtain permission to attack.[28]

There are a number of technical and legal issues with weapons such as the WASAAMM.[29] While most of the engineering aspects of such a weapon are likely to be achievable in the next twenty-five years, the 'autonomous' part of the weapon still poses significant engineering issues. In addition, there are issues with achieving compliance with international humanitarian law, and resulting rules of engagement, that are yet to be resolved.[30] Of course, if the WASAAMM operated in the mode where it relayed a signal to obtain permission to attack,[31] that would significantly reduce the engineering and international humanitarian law (and rules of engagement) compliance issues – but it also would not be a true autonomous weapon if operating in that mode.

An area that is related to autonomous weapons is the development of artificial intelligence assistants to help humans shorten the observe, orient, decide, act (OODA) loop. The purpose of such decision-support systems is to address the fact that while 'speed-ups in information gathering and distribution can be attained by well-implemented networking, information analysis, understanding and decision making can prove to be severe bottlenecks to the operational tempo'.[32] There is very

27 Chris Anzalone, 'Readying air forces for network centric weapons', 2003, slide 9, available at: http://www.dtic.mil/ndia/2003targets/anz.ppt (last visited 8 May 2012).

28 US Air Force, 'Transformation flight plan', 2003, Appendix D, p. 11, available at: http://www.au.af.mil/au/awc/awcgate/af/af_trans_flightplan_nov03.pdf (last visited 8 May 2012).

29 Myers also discusses some of the moral aspects, e.g., is it 'morally correct for a machine to be able to take a life'? See A. Myers, above note 23, pp. 87–88. See also ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, Report of the 31st International Conference of the Red Cross and Red Crescent, 2011, p. 40. Moral issues are also discussed in Kenneth Anderson and Matthew Waxman, 'Law and ethics for robot soldiers', in *Policy Review* (forthcoming 2012), available at: http://ssrn.com/abstract=2046375 (last visited 8 May 2012). See generally Peter Singer, 'The ethics of killer applications: why is it so hard to talk about morality when it comes to new military technology?', in *Journal of Military Ethics*, Vol. 9, No. 4, 2010, pp. 299–312.

30 *Ibid.*

31 For example, the UK 'Fire Shadow' will feature: 'Man In The Loop (MITL) operation, enabling a human operator to overrule the weapon's guidance and divert the weapon's flight path or abort the attack and return to loiter mode in conditions where friendly forces are at risk, prevailing conditions do not comply with rules of engagement, or where an attack could cause excessive collateral damage', see 'Fire Shadow: a persistent killer', Defense Update, 2008, available at: http://defense-update.com/20080804_fire-shadow-a-persistent-killer.html (last visited 8 May 2012).

32 Shyni Thomas, Nitin Dhiman, Pankaj Tikkas, Ajay Sharma and Dipti Deodhare, 'Towards faster execution of the OODA loop using dynamic decision support', in Leigh Armistead (ed.), *The 3rd International Conference on Information Warfare and Security*, 2008, p. 42, available at: http://academic-conferences.org/pdfs/iciw08-booklet-A.pdf (last visited 8 May 2012).

limited publicly available information on how such decision-support systems might operate in the area of targeting.

The key issue is how to use 'computer processing to attempt to automate what people have traditionally had to do'.[33] Using sensors and computer power to periodically scan an airfield for changes, and thereby cue a human analyst, has been more successful than using sensors such as synthetic aperture radar to provide automatic target recognition.[34] A clear difficulty is that the law relating to targeting is generally expressed in broad terms with a range of infinitely varying facts, rather than as precise formulas with constrained variables, which is why a commander's judgement is often needed when determining whether an object or person is subject to lawful attack.[35] As Taylor points out, it is this 'highly contextual nature' of targeting that results in there not being a simple checklist of lawful targets.[36] However, if a commander was prepared to forgo some theoretical capability, it is possible in a particular armed conflict to produce a subset of objects that are at any given time targetable. As long as the list is maintained and reviewed, at any particular moment in an armed conflict it is certainly possible to decide that military vehicles, radar sites, etcetera are targetable. In other words, a commander could choose to confine the list of targets that are subject to automatic target recognition to a narrow list of objects that are clearly military objectives by their nature – albeit thereby forgoing automatic target recognition of other objects that require more nuanced judgement to determine status as military objectives through their location, purpose, or use.[37]

The next step is to move beyond a system that is programmed to be a system that, like a commander, learns the nature of military operations and how to apply the law to targeting activities. As communication systems become more complex, not 'only do they pass information, they have the capacity to collate, analyse, disseminate . . . and display information in preparation for and in the prosecution of military operations'.[38] Where a system is 'used to analyse target data and then provide a target solution or profile'[39] then the 'system would reasonably

33 See above note 24, p. 47.

34 *Ibid.*, pp. 47–48. Automatic target recognition systems have worked in the laboratory but have not proved reliable when deployed and presented with real data rather than 'unrealistic controlled data for assessing the performance of algorithms', *ibid.*, pp. 47 and 53. While now somewhat dated, an article that explains how such target recognition works is Paul Kolodzy, 'Multidimensional automatic target recognition system evaluation', in *The Lincoln Laboratory Journal*, Vol. 6, No. 1, 1993, p. 117.

35 See C. Taylor, above note 15, p. 9. See generally Ian Henderson, *The Contemporary Law of Targeting: Military Objectives, Proportionality and Precautions in Attack under Additional Protocol I*, Martinus Nijhoff, Leiden, 2009, pp. 45–51.

36 See C. Taylor, *ibid.*, p. 9; see also I. Henderson, *ibid.*, pp. 49–50.

37 See above note 1, Art. 52(2) of API.

38 See J. McClelland, above note 1, p. 405. The technical issues (from as simple as meta-data standards for the sensor-collected data and available bandwidth for transmission of data, through to the far more complex) should not be downplayed, particularly with multi-sensor data. See generally, *Report of the Joint Defense Science Board Intelligence Science Board Task Force on Integrating Sensor-Collected Intelligence*, above note 24, pp. 1–9.

39 See J. McClelland, above note 1, p. 405.

fall within the meaning of "means and methods of warfare" as it would be providing an integral part of the targeting decision process'.[40]

What might a system look like that does not require detailed programming but rather learns? Suppose an artificial intelligence system scans the battlespace and looks for potential targets (let's call it the 'artificial intelligence target recognition system' (AITRS)). Rather than needing to be preprogrammed, the AITRS learns the characteristics of targets that have previously been approved for attack.[41] With time, the AITRS gets better at excluding low-probability targets and better at cueing different sensors and applying algorithms to defeat the enemy's attempt at camouflage, countermeasures, etcetera. In one example, the outcome of the process is that the AITRS presents a human operator with a simplified view of the battlespace where only likely targets and their characteristics are presented for human analysis and decision whether to attack. Importantly though, all of the 'raw information' (e.g., imagery, multispectral imagery, voice recordings of intercepted conversations, etcetera) is available for human review. In example two, while the AITRS still presents a human operator with a simplified view of the battlespace with likely targets identified for approval to attack, the human decision-maker is not presented with 'raw information' but rather analysed data.[42] For example, the human might be presented with a symbol on a screen that represents a motor vehicle along with the following:

- probability of one human rider: 99 per cent
- probability of body-match to Colonel John Smith:[43] 75 per cent
- probability of voice-match to Colonel John Smith: 90 per cent.[44]

And finally, in example three it is the AITRS itself that decides whether to prosecute an attack. Assuming the AITRS is also linked to a weapon system then the combination is an autonomous weapon system.

It would seem beyond current technology to be able to program a machine to make the complicated assessments required to determine whether or not a particular attack would be lawful if there is an expectation of collateral

40 *Ibid.*, p. 406.

41 See K. Anderson and M. Waxman, above note 29, p. 10.

42 'Automatically processing the sensor data to reduce critical information to a smaller data packet or to provide a go/no-go response could improve reaction time', in *Report of the Joint Defence Science Board Intelligence Science Board Task Force on Integrating Sensor-Collected Intelligence*, above note 24, p. 43.

43 Assume Colonel Smith is a person on the high-value target list and issues such as *hors de combat* (e.g., wounded, sick, surrendering, or otherwise out of combat) and collateral damage aside, is otherwise subject to lawful attack. This type of attack is based on identifying a target as being Colonel Smith. Contrast this with attacks based on characteristics of the target that are associated with 'enemy forces' (such as unloading explosives, gathering at certain locations, and other patterns of behaviour) without knowing the actual identity of the target. The latter are becoming known as 'signature' strikes, while the former are 'personality' strikes. See Greg Miller, 'CIA seeks new authority to expand Yemen drone campaign', in *The Washington Post*, 19 April 2012, available at: http://www.washingtonpost.com/world/national-security/cia-seeks-new-authority-to-expand-yemen-drone-campaign/2012/04/18/gIQAsaumRT_story.html (last visited 6 May 2012).

44 See also the example used by Myers, and his discussion of multi-sensor cueing. A. Myers, above note 23, p. 84.

damage.[45] Indeed, one would wonder even where to start as assessing anticipated military advantage against expected collateral damage is like comparing apples and oranges.[46] For now, that would mean any such weapon system should be employed in such a manner as to reduce the risk of collateral damage being expected.[47] However, a true AITRS that was initially operated with human oversight could presumably 'learn' from the decisions made by its human operators on acceptable and unacceptable collateral damage.[48]

As pointed out at footnote 46 above, collateral damage assessments are not just about calculating and comparing numbers – a function well suited to current computers. But instead, there is a clear qualitative assessment, albeit one where the things being compared are not even alike. How could a machine ever make such judgements? Perhaps not through direct programming but rather by pursuing the artificial intelligence route. So, along with learning what are lawful targets, our hypothetical AITRS would also learn how to make a proportionality assessment in the same way humans do – through observation, experience, correction in the training environment (e.g., war games), and so on. An AITRS that failed to make reasonable judgements (in the view of the instructing staff) might be treated the same as a junior officer who never quite makes the grade (perhaps kept on staff but not given decision-making authority), whereas an AITRS that proved itself on course and in field exercises could be promoted, entrusted with increasing degrees of autonomy, etcetera.

Another technical problem is that the required identification standard for determining whether a person or object is a lawful target is not clear-cut. The standard expressed by the International Criminal Tribunal for the Former Yugoslavia is that of 'reasonable belief'.[49] In their rules of engagement, at least two states have adopted the standard of 'reasonable certainty'.[50] A third approach,

45 ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, above note 29, pp. 39–40; William Boothby, *Weapons and the Law of Armed Conflict*, Oxford University Press, Oxford, 2009, p. 233.

46 See I. Henderson, above note 35, pp. 228–229. Many facets of military operations require commanders to exercise judgement, and this includes certain legal issues. Having determined what is the military advantage expected from an attack (not an exact quantity in itself) on a command and control node, and estimated the expected incidental civilian injury, death, and damage, somehow these two factors must be compared. The evaluation is clearly somewhat subjective and likely to differ from person to person, rather than objective and mathematical. In this respect, one can think of interpreting and complying with certain aspects of international humanitarian law as part art and not just pure science.

47 W. Boothby, above note 45, p. 233.

48 For a contrary view, see Markus Wagner, 'Taking humans out of the loop: implications for international humanitarian law', in *Journal of Law Information and Science*, Vol. 21, 2011, p. 11, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1874039 (last visited 8 May 2012), who concludes that autonomous systems will never be able to comply with the principle of proportionality.

49 'The Trial Chamber understands that such an object [normally dedicated to civilian purposes] shall not be attacked when it is not reasonable to believe, in the circumstances of the person contemplating the attack, including the information available to the latter, that the object is being used to make an effective contribution to military action', ICTY, *The Prosecutor v Galic*, Case No IT-98-29-T, Judgement (Trial Chamber), 5 December 2003, para. 51.

50 International and Operational Law Department: The Judge Advocate General's Legal Centre & School (US Army), *Operational Law Handbook 2012,* 'CFLCC ROE Card', p. 103, available at: http://www.loc.gov/rr/frd/Military_Law/operational-law-handbooks.html (last visited 8 May 2012); ICRC, *Customary IHL*,

reflected in the San Remo *Rules of Engagement Handbook* is to require identification by visual and/or certain technical means.[51] The commander authorizing deployment of an autonomous weapon, and any operator providing overwatch of it, will need to know what standard was adopted to ensure that both international law and any operation-specific rules of engagement are complied with. It is also possible to combine the requirement for a particular level of certainty (e.g., reasonable belief or reasonable certainty) with a complementary requirement for identification to be by visual and/or certain technical means.

Presumably, for any identification standard to be able to be coded[52] into a computer program that standard would need to be turned into a quantifiable confirmation expressed as a statistical probability. For example, 'reasonable belief' would need to be transformed from a subjective concept into an objective and measurable quantity – for example, '95 per cent degree of confidence'. This would then be used as the benchmark against which field experience (including historical data) could produce an empirical equation to profile a potential target. Then new battlespace data can be compared to quantify (assess) the strength of correlation to the required degree of confidence (in the current example, 95 per cent or greater correlation). However, the uncertainty of measurement associated with the battlespace feedback sensors would also need to be quantified as a distinctly separate acceptance criterion. For example, assume in certain operational circumstances that an uncertainty of measurement results in an uncertainty of plus or minus 1 per cent, whereas in other operational circumstances the uncertainty is plus or minus 10 per cent. In the first circumstance, to be confident of 95 per cent certainty, the correlation would need to be not less than 96 per cent. In the second case, though, the required degree of confidence would never be achievable as the required degree of confidence of 95 per cent cannot be achieved due to the measurement uncertainty.[53]

Methods for the lawful employment of automated and autonomous weapons

Most weapons are not unlawful as such – it is how a weapon is used and the surrounding circumstances that affect legality.[54] This applies equally to automated and autonomous weapons, unless such weapons were to be banned by treaty

'Philippines: Practice Relating to Rule 16. Target Verification', 2012, available at: http://www.icrc.org/customary-ihl/eng/docs/v2_cou_ph_rule16 (last visited 8 May 2012).

51 See the sample rules at Series 31 'Identification of Targets', in International Institute of Humanitarian Law, *Rules Of Engagement Handbook*, San Remo, 2009, p. 38.

52 Again, a non-coding method would be through artificial intelligence.

53 In this second case, the targeting system could provide cueing for other sensors or a human operator; it just would be programmed to not permit autonomous weapon release.

54 Philip Spoerri, 'Round table on new weapon technologies and IHL – conclusions', in *34th Round Table on Current Issues of International Humanitarian Law*, San Remo, 8–10 September 2011, available at: http://www.icrc.org/eng/resources/documents/statement/new-weapon-technologies-statement-2011-09-13.htm (last visited 8 May 2012).

(e.g., like non-command-detonated anti-personnel landmines). There are various ways to ensure the lawful employment of such weapons.

> [The] absence of what is called a 'man in the loop' does not necessarily mean that the weapon is incapable of being used in a manner consistent with the principle of distinction. The target detection, identification and recognition phases may rely on sensors that have the ability to distinguish between military and non-military targets. By combining several sensors the discriminatory ability of the weapon is greatly enhanced.[55]

One method of reducing the target recognition and programming problem is to not try to achieve the full range of targeting options provided for by the law. For example, a target recognition system might be programmed to only look for high-priority targets such as mobile air defence systems and surface-to-surface rocket launchers – objects that are military objectives by nature and, therefore, somewhat easier to program as lawful targets compared to objects that become military objectives by location, purpose, or use.[56] As these targets can represent a high priority, the targeting software might be programmed to only attack these targets and not prosecute an attack against an otherwise lawful target that was detected first but is of lower priority.[57] If no high-priority target is detected, the attack could be aborted or might be prosecuted against other targets that are military objectives by nature. Adopting this type of approach would alleviate the need to resolve such difficult issues as how to program an autonomous system to not attack an ambulance except where that ambulance has lost protection from attack due to location, purpose, or use.[58]

A further safeguard includes having the weapon '"overwatched" and controlled remotely, thereby allowing for it to be switched off if considered potentially dangerous to non-military objects'.[59] Such overwatch is only legally (and operationally) useful if the operators provide a genuine review and do not simply trust the system's output.[60] In other words, the operator has to value add. For example, if an operator is presented with an icon indicating that a hostile target has been identified, then the operator would be adding to the process if that person separately considered the data, observed the target area for the presence of civilians, or in some other way did more than simply authorize or prosecute an attack based on the analysis produced by the targeting software. In other words, the operator

55 J. McClelland, above note 1, pp. 408–409.

56 See Lockheed Martin, 'Low cost autonomous attack system', in *Defense Update,* 2006, available at: http://defense-update.com/products/l/locaas.htm (last visited 8 May 2012).

57 An example would be detecting a T-72 tank but ignoring it as a low-priority target and continuing in search mode until detecting and engaging an SA-8 mobile surface-to-air missile launcher, *ibid.*

58 The presumption being that the high-priority targets are all clearly military in nature and, therefore, it would be easier to program target recognition software to identify such targets. If the high-priority targets happened to be ambulances being misused as mobile command and control vehicles, programming issues would still remain. See above note 37 and the accompanying text.

59 J. McClelland, above note 1, pp. 408–409.

60 See *Report of Defense Science Board Task Force on Patriot System Performance: Report Summary*, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2005, p. 2.

is either double-checking whether the target itself may be lawfully attacked, or is ensuring that the other precautions in attack (minimizing collateral damage, assessing any remaining collateral damage as proportional, issuing a warning to civilians where required, etcetera) are being undertaken. A problem arises where the operator is provided with large volumes of data,[61] as his or her ability to provide meaningful oversight could be compromised by information overload.[62] A way to manage this would be for the targeting software to be programmed in such a way that the release of a weapon is recommended only when the target area is clear of non-military objects.[63] In other circumstances, the targeting software might simply identify the presence of a target and of non-military objects and not provide a weapon release recommendation, but only a weapon release solution. In other words, the targeting software is identifying how a particular target could be hit, but is neutral on whether or not the attack should be prosecuted, thereby making it clear to the operator that there are further considerations that still need to be taken into account prior to weapon release.

Two further legal aspects of automated and autonomous weapons (and remotely operated weapons) that require further consideration are the rules relating to self-defence[64] and how the risk to own forces is considered when assessing the military advantage from an attack and the expected collateral damage.

The issue of self-defence has two aspects: national self-defence (which is principally about what a state can do in response to an attack) and individual self-defence (which is principally about what an individual can do in response to an attack).[65] Prior to an armed conflict commencing, the first unlawful use of force against a state's warships and military aircraft may be considered as amounting to an armed attack on that state, thereby allowing it to invoke the right of national self-defence. Would the same conclusion be reached if the warship or military aircraft were unmanned? Imagine an attack on a warship that for whatever reason had none of the ship's company on board at the time of the attack. What is it about attacks on warships that is of legal significance: the mere fact that it is a military vessel that is flagged to the state, the likelihood that any attack on the warship also imperils the ship's company, or a combination of the two?

Second, consider the different legal authorities for using lethal force. In broad terms, individual self-defence allows Person A to use lethal force against Person B when Person B is threatening the life of Person A.[66] Whether Persons A and B are opposing enemy soldiers or not is an irrelevant factor. Compare this to international humanitarian law, which allows Soldier A to use lethal force against

61 This could be a single system that processes and displays large volumes of data or a single operator who is given multiple systems to oversee.
62 ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, above note 29, p. 39.
63 J. McClelland, above note 1, pp. 408–409.
64 Conversations between Patrick Keane and Ian Henderson, 2011–2012.
65 In this context, individual self-defence also encompasses the issue of defending another party against an unlawful attack.
66 Domestic criminal law varies from jurisdiction to jurisdiction and the issue is more nuanced than this simple explanation.

Soldier B purely because Soldier B is the enemy.[67] Soldier B need not be posing any direct threat to Soldier A at all. Indeed, Soldier B may be asleep and Soldier A might be operating a remotely piloted armed aircraft. However, Soldier A must be satisfied, to the requisite legal standard, that the target is in fact an enemy soldier. Identification, not threat, is the key issue. However, during rules of engagement briefings military members are taught that during an armed conflict not only can they fire upon identified enemy, but also that nothing in international humanitarian law (or other law for that matter) prevents them from returning fire against an unidentified[68] contact in individual self-defence.[69] This well-known mantra will require reconsideration when briefing operators of unmanned assets. In all but the most unusual of circumstances, the remote operator of an unmanned asset will not be personally endangered if that unmanned asset is fired upon. This issue will need to be carefully considered by drafters of rules of engagement and military commanders, as generally returning fire to protect only equipment (and not lives) would be illegal under the paradigm of individual self-defence.[70] Compare this to the international humanitarian law paradigm that arguably would allow use of lethal force to protect certain types of property and equipment from attack, based on an argument that whoever is attacking the property and equipment must be either (1) an enemy soldier, or (2) a civilian taking a direct part in hostilities.[71]

Similarly, how to treat an unmanned asset under international humanitarian law when considering the 'military advantage' to be gained from an attack is not straightforward. While risk to attacking forces is a factor that can be legitimately considered as part of the military advantage assessment,[72] traditionally that has been thought of as applying to the combatants and not the military equipment. While it is logical that risk of loss of military equipment is also a factor, it will clearly be a lesser factor compared with risk to civilian life.

In conclusion, it is the commander who has legal responsibility 'for ensuring that appropriate precautions in attack are taken'.[73] Regardless of how remote in time or space from the moment of an attack, individual and state responsibility attaches to those who authorize the use of an autonomous weapon system.[74] It should be noted that this does not mean a commander is automatically

67 Subject to Soldier B being *hors de combat*. It would also be lawful under international humanitarian law for Soldier A to fire upon Person B for such time as Person B was a civilian taking a direct part in hostilities, but space does not allow a further exploration of that point.

68 Unidentified in the sense of unaware whether the person firing is an enemy soldier, a civilian, etcetera. There is still a requirement to identify the source (i.e., the location) of the threat.

69 The concept of 'unit self-defence' adds little to the present discussion, being a blend of both national and individual self-defence.

70 The legal paradigm of individual self-defence can be invoked to protect equipment where loss of that equipment would directly endanger life.

71 As long as I am satisfied that I have at least one legal basis for using lethal force against a *person (e.g.,* enemy combatant of civilian taking a direct part in hostilities), I do not have to determine which one is actually the case. Space does not allow a full discussion of this point, or the other interesting issue of using force to protect equipment as part of a national security interest under national self-defence outside of an armed conflict.

72 I. Henderson, above note 35, p. 199.

73 C. Taylor, above note 15, p. 12.

74 P. Spoerri, above note 54.

liable if something goes wrong. In war, accidents happen. The point under discussion is who could be found liable, not who is guilty.

The above discussion has focused on the intended target of a weapon. The following discussion deals with emerging weapons that highlight the legal issue of weapon effect even where the target is an otherwise lawful target.

Weapon effect

Directed energy weapons

Directed energy weapons use the electromagnetic spectrum (particularly ultraviolet through to infrared and radio-frequency (including microwave)) or sound waves to conduct attacks.[75] As a means of affecting enemy combat capability, directed energy weapons can be employed directly against enemy personnel and equipment, or indirectly as anti-sensor weapons. For example, laser systems could be employed as 'dazzlers' against aided and unaided human eyesight, infrared sensors, and space-based or airborne sensors,[76] and as anti-equipment weapons.[77] High-powered microwaves can be employed against electronic components and communications equipment. Lasers and radars are also used for target detection, target tracking, and finally for providing target guidance for other conventional weapons.

When directed energy weapons are employed against enemy communication systems, the legal issues are not significantly different from those that would arise if kinetic means were used. Is the target (e.g., a communication system) a lawful military objective and have incidental effects on the civilian population been assessed? As directed energy weapons have the clear potential to reduce the immediate collateral effects commonly associated with high-explosive weapons (e.g., blast and fragmentation),[78] the main incidental effect to consider is the second-order consequences of shutting down a communication system such as air traffic control or emergency services. While it is common to state that second-order effects must be considered when assessing the lawfulness of an attack, a proper understanding of what is 'counted' as collateral damage for the purpose of proportionality assessments is required. It is a mistake to think that any inconvenience caused to the civilian population must be assessed. That is wrong.

75 Particle weapons are also being studied but currently appear to remain in the area of theory, see Federation of American Scientists, 'Neutral particle beam', 2012, available at: http://www.fas.org/spp/starwars/program/npb.htm (last visited 8 June 2012); Carlo Popp, 'High energy laser directed energy weapons', 2012, available at: http://www.ausairpower.net/APA-DEW-HEL-Analysis.html (last visited 8 June 2012). For a good review of 'non-lethal' directed energy weapons (including acoustic weapons), see Neil Davison, *'Non-Lethal' Weapons*, Palgrave MacMillan, Basingstoke, 2009, pp. 143–219.

76 Laser systems could be employed as 'dazzlers' against space-based or airborne sensors while high-powered microwaves can be employed against electronic components, see *Defense Science Board Task Force on Directed Energy Weapons*, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, US Department of Defense, December 2007, pp. 2, 11 and 13.

77 Particularly for use against missiles, mine-clearing and as anti-satellite weapons, *ibid.*, p. 19.

78 As do other kinetic weapons such as inert concrete bombs.

Along with death and injury, it is only 'damage' to civilian objects that must be considered.[79] Therefore, a directed energy weapon attack on an air traffic control system that affected both military and civilian air traffic[80] need only consider the extent to which civilian aircraft would be damaged, along with associated risk of injury or death to civilians, and need not consider mere inconvenience, disruption to business, etcetera.[81]

Directed energy weapons are also being developed as non-lethal (also known as less-lethal) weapons to provide a broader response continuum for a controlled escalation of force.[82] For a variety of operational and legal reasons, it is preferable to have an option to preserve life while still achieving a temporary or extended incapacitation of the targeted individual. However, the very terms used to describe these weapons can cause problems beyond any particular legal or policy constraints.[83] The unintended consequences of the weapons (particularly due to the unknown health characteristics of the target) can lead to permanent injury or death. Such consequences are then used to stigmatize the concept of a non-lethal/less-than-lethal weapon. The important point to remember is that as for any other combat capability (including kinetic weapons), use of directed energy weapons during an armed conflict is governed by international humanitarian law and by any applicable rules of engagement and directions from the combat commander.[84]

Non-lethal directed energy weapons can be used in combination with traditional, lethal weapons. For example, it is reported that:

> Another weapon . . . can broadcast deafening and highly irritating tones over great distances. The long-range device precisely emits a high-energy acoustic beam as far as five football fields away. To a reporter standing across the airstrip from where it was set up in a hangar here, it sounded as if someone was shouting directly into his ear.
>
> The device 'has proven useful for clearing streets and rooftops during cordon and search . . . and for drawing out enemy snipers who are subsequently destroyed by our own snipers', the 361st Psychological Operations Company, which has tested the system in Iraq, told engineers in a report.[85]

79 See above note 1, Art. 51(5)(b) and Art. 57(2)(a)(iii) of API.

80 See ICRC, 'Cyber warfare and IHL: some thoughts and questions', 2011, available at: http://www.icrc.org/eng/resources/documents/feature/2011/weapons-feature-2011-08-16.htm (last visited 8 May 2012).

81 Space does not permit a full discussion of this point, but other factors warranting discussion are effects on neutrals and any third-order affects (e.g., the effect on emergency health-care flights), although query whether the 'ICRC might have a role in helping to generate international consensus on whether civilians have fundamental rights to information, electrical power, etc., in the same way as they have rights to life and property', *ibid.*

82 See generally, US Department of Defense, 'Non-lethal weapons program', available at: http://jnlwp.defense.gov/index.html (last visited 8 May 2012); James Duncan, 'A primer on the employment of non-lethal weapons', in *Naval Law Review*, Vol. XLV, 1998. See also Jürgen Altmann, 'Millimetre waves, lasers, acoustics for non-lethal weapons? Physics analyses and inferences', in DSF-Forschung, 2008, available at: http://www.bundesstiftung-friedensforschung.de/pdf-docs/berichtaltmann2.pdf (last visited 8 May 2012).

83 See *Defense Science Board Task Force on Directed Energy Weapons*, above note 76, p. xii.

84 *Ibid.*, p. xiii.

85 Bryan Bender, 'US testing nonlethal weapons arsenal for use in Iraq', in *Boston Globe*, 5 August 2005, available at: http://www.boston.com/news/nation/articles/2005/08/05/us_testing_nonlethal_weapons_

This form of directed energy weapon demonstrates two key issues associated with non-lethal weapon technology. First, such weapons are likely to be used against a civilian population – in this case, to clear streets and rooftops.[86] Second, the non-lethal weapon may be employed in conjunction with existing weapons to achieve a lethal effect.

Other directed energy weapons include active denial systems.[87]

> One of the weapons that has been successfully tested is a heat beam . . . that can 'bake' a person by heating the moisture in the first one-64th of an inch of the epidural layer of the skin. It was originally developed for the Department of Energy to keep trespassers away from nuclear facilities.[88]

The 'irresistible heating sensation on the adversary's skin [causes] an immediate deterrence effect';[89] because the heating sensation causes 'intolerable pain [the body's] natural defense mechanisms take over'.[90] The 'intense heating sensation stops only if the individual moves out of the beam's path or if the beam is turned off'.[91] Because flamethrowers and other incendiary weapons are only regulated and not specifically banned by international humanitarian law, there is no legal reason to deny the use of the active denial system in combat.[92]

Where active denial systems are being used as an invisible 'fence', then clearly it is a matter for the individual as to whether to approach the fence, and if so, whether to try to breach the perimeter.[93] However, if active denial systems are being aimed at a person or group to clear an area,[94] an issue that needs consideration with this type of weapon is how would a person who is being subjected to this type of attack either surrender or consciously choose to leave an area when they can neither see the beam,[95] may be unaware of even this type of technology, and are reacting to intolerable pain like the 'feeling . . . [of] touching a hot frying pan'?[96] Reacting

arsenal_for_use_in_iraq/?page=full (last visited 8 June 2012). The Long Range Acoustic Device is described in detail in Altmann, above note 82, pp. 44–53. As Altmann notes, while described as a hailing or warning device, it can potentially be used as a weapon, *ibid*., p. 52. For a discussion on attempts to avoid the legal requirement to review new 'weapons' by describing these types of acoustic devices by other names, see N. Davison, above note 75, pp. 102 and 205.

86 Concerns about using non-lethal weapons against the civilian population, or against 'individuals before it is ascertained whether or not they are combatants' are raised in Davison, above note 75, pp. 216–217.

87 *Defense Science Board Task Force on Directed Energy Weapons*, note 76, pp. 33 and 38. For more details see 'Active denials system demonstrates capabilities at CENTCOM', United State Central Command, available at: http://www.centcom.mil/press-releases/active-denial-system-demonstrates-capabilities-at-centcom (last visited 8 May 2012).

88 B. Bender, above note 85. The Active denial system is described in detail in J. Altmann, above note 82, pp. 14–28.

89 *Defense Science Board Task Force on Directed Energy Weapons*, above note 76, p. 38.

90 *Ibid.*, p. 42.

91 *Ibid.*

92 J. Altmann, above note 82, p. 27.

93 Conversation between Patrick Keane and Ian Henderson, 14 April 2012.

94 As opposed to traditional kinetic weapons where the desired effect is to disable (through either wounding or killing).

95 See J. Altmann, above note 82, p. 28.

96 *Defense Science Board Task Force on Directed Energy Weapons*, above note 76, p. 42.

instinctively to intolerable pain seems likely to make a person incapable of rational thought.[97] Employment of such weapons will need to be well regulated through a combination of the tactics, techniques and procedures, and rules of engagement to ensure that unnecessary suffering is not caused through continued use of the weapon because a person has not cleared the target area.[98] In this respect, and noting that the active denial system has 'successfully undergone legal, treaty and US Central Command rules of engagement reviews',[99] it is worth recalling that as states' legal obligations vary, and as states may employ weapons differently, the legal review by one state is not determinative of the issue for other states.[100] This may prove interesting in the sale of highly technical equipment, as the details of a weapon's capability are often highly classified and compartmentalized. The state conducting the review may not control access to the necessary data. As discussed below, this may require lawyers, engineers, and operators to work together cooperatively and imaginatively to overcome security classification and compartmental access limitations.

A similar directed energy weapon using different technology is 'a high-powered white light so intense as to send any but the most determined attackers running in the opposite direction'.[101] Concepts for employment of the weapon appear to include using it as a means to identify hostile forces, as evidenced by the statement: 'If anyone appears willing to withstand the discomfort, "I know your intent", [Colonel Wade] Hall [a top project official] said. "I will kill you."'[102] While initially such statements appear quite concerning, it is instructive to consider whether this is in reality any different from the 'traditional' warnings and escalation of force scenarios such as 'stop or I will shoot' or employment of flares and dazzlers to warn vehicles not to approach too close to military convoys.

Where directed energy weapons are used to counter (often improvised) explosive devices,[103] the issue is primarily about consequences. If the directed energy weapon is causing a detonation at a safe range from friendly forces, there is a requirement to consider whether any civilians or other non-combatants are in the vicinity of the detonation and, therefore, at risk of injury or death.[104]

97 Email April-Leigh Rose/Ian Henderson, 24 April 2012.
98 Altmann also recommends investigating risk to eyesight due to potential damage to the cornea; see J. Altmann, above note 82, p. 28.
99 *Ibid.*, p. 38.
100 See J. McClelland, above note 1, p. 411, who makes this point with respect to manufacturer's claims of legality.
101 B. Bender, above note 85.
102 *Ibid.*
103 See *Defense Science Board Task Force on Directed Energy Weapons*, above note 76, p. 40.
104 Space does not permit a full exploration of this point, but note that the issues are different if instead of causing a detonation the countermeasure prevents the explosive device from detonating.

Cyber operations

Cyber operations are:

> operations against or via a computer or a computer system through a data stream.[105] Such operations can aim to do different things, for instance to infiltrate a system and collect, export, destroy, change, or encrypt data or to trigger, alter or otherwise manipulate processes controlled by the infiltrated computer system. By these means, a variety of 'targets' in the real world can be destroyed, altered or disrupted, such as industries, infrastructures, telecommunications, or financial systems.[106]

Cyber operations are conducted via software, hardware, or via a combination of software and personnel. A recent example of a cyber operation that was essentially conducted purely by software is the Stuxnet virus. Once in place, the Stuxnet virus appears to have operated independently of any further human input.[107] Compare this to a software program that is designed to allow a remote operator to exercise control over a computer – allowing, among other things, the upload of data or modification of data on the target computer. Finally, a non-military example of a cyber operation that requires both hardware and software is credit card skimming.

The application of specific international humanitarian law rules to cyber warfare remains a topic of debate.[108] However, for the purposes of this article, it is assumed that the key international humanitarian law principles of distinction, proportionality, and precaution, apply, as a minimum, to those cyber attacks that have physical consequences (e.g., the Stuxnet virus altered the operating conditions for the Iranian uranium enrichment centrifuges, which ultimately resulted in physical damage to those centrifuges).[109] Four particular legal aspects of cyber weapons are worth mentioning.

First, cyber weapons have the distinct possibility of being operated by civilians.[110] The 'weapon' is likely to be remote from the battlefield, is technologically sophisticated, and does not have an immediate association with death and injury. The operation of the cyber weapon exposes a civilian operator to

105 Based on this definition, a kinetic attack to shut down a computer system (for example, by dropping a bomb on the building housing the computer) would not be a cyber operation.

106 ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, above note 29, p. 36.

107 See Angus Batey, 'The spies behind your screen', in *The Telegraph*, 24 November 2011; Jack Goldsmith, 'Richard Clarke says Stuxnet was a US operation', in *LawFare: Hard National Security Choices*, 29 March 2012, available at: http://www.lawfareblog.com/2012/03/richard-clarke-says-stuxnet-was-a-u-s-operation/ (last visited 18 April 2012).

108 See 'Tallinn Manual on the International Law Applicable to Cyber Warfare', 2012, pp. 17–22, available at: http://issuu.com/nato_ccd_coe/docs/tallinn_manual_draft/23 (last visited 8 June 2012).

109 ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, above note 29, pp. 36–37.

110 See Adam Segal, 'China's cyber stealth on new frontline', in the *Australian Financial Review*, 30 March 2012, available at: http://afr.com/p/lifestyle/review/china_cyber_stealth_on_ new_frontline_z6YvFR0mo3uC87zJvCEq6H (last visited 1 June 2012), referring to 'cyber-militias' at technology companies recruited by the People's Liberation Army.

lethal targeting (as a civilian taking a direct part in hostilities),[111] as well as potential criminal prosecution for engaging in acts not protected by the combatant immunity enjoyed by members of the armed forces.[112] These issues are discussed in detail in a recent article by Watts who raises, among other things, the possibility of the need for a complete rethink of how the law on direct participation in hostilities applies in the area of cyber warfare.[113] It could also be queried what training such civilian operators might have in the relevant rules of international humanitarian law.[114]

Second, cyber attacks can have consequences in the real world and not just the virtual world.[115] Where those consequences affect the civilian population by causing loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, those consequences must be considered under international humanitarian law.[116] The discussion of this point for directed energy weapon attacks applies equally to cyber attacks. A further related consideration is that where it could reasonably be expected that a virus introduced into a military system might find its way into civilian systems and cause infrastructure damage, that collateral damage must also be considered.[117] A common example of a possible cyber attack that would directly affect civilians is disabling a power station – either just by shutting it down, or by overloading or shutting down a fail-safe, thereby damaging hardware. This can potentially happen to any infrastructure maintained by software.

Third, cyber weapons need to be considered not only in relation to international humanitarian law, but also very importantly under *jus ad bellum*.[118] As Blake and Imburgia point out, even if a cyber attack has no kinetic effects, the attack might still be contrary to the UN Charter specifically or international law generally[119] and may, if amounting to an 'armed attack', legitimize the use of force by the affected state in self-defence.

111 See above note 1, Article 51(3) of API.

112 On both these points, see D. Blake and J. Imburgia, above note 1, pp. 195–196.

113 See Sean Watts, 'Combatant status and computer network Attack', in *Virginia Journal of International Law*, Vol. 50, No. 2, 2010, p. 391.

114 See J. Kellenberger, above note 15, where this point was made with respect to remotely operated weapon systems.

115 ICRC, 'Cyber warfare and IHL: some thoughts and questions', above note 80.

116 See above note 1, Art. 51(5)(b) and Art. 57(2)(a)(iii) of API. It is a matter of policy whether to consider other consequences for the civilian population such as disruption, loss of amenities, etcetera.

117 See ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, above note 29, p. 38.

118 Put simply, *jus ad bellum* is the law regulating the overall resort to the use of force, compared to international humanitarian law (*jus in bello*) that regulates the individual instances of the application of force during an armed conflict. See Matthew Waxman, 'Cyber attacks as "force" under UN Charter Article 2(4)', in Raul Pedrozo and Daria Wollschlaeger (eds), *International Law and the Changing Character of War, International Law Studies*, Vol. 87, 2011, p. 43; Sean Watts, 'Low-intensity computer network attack and self-defense', in *ibid*., p. 59; Michael Schmitt, 'Cyber operations and the *jus ad bellum* revisited', in *Villanova Law Review*, Vol. 56, No. 3, 2011, pp. 569–605.

119 D. Blake and J. Imburgia, above note 1, pp. 184–189. Discussed in more detail in M. Schmitt, *ibid.*, who also discusses the current 'fault lines in the law governing the use of force [that] have appeared because it is a body of law that predates the advent of cyber operations'.

Finally, the very nature of cyber warfare can make it hard to determine who initiated an attack, and issues of attribution go to the very heart of both state responsibility and individual accountability.[120]

Nanotechnology and weaponization of neurobiology

> Nano-weapons are hard to define, but encompass not only objects and devices using nanotechnology that are designed or used for harming humans, but also those causing harmful effects in nano-scale if those effects characterise the lethality of the weapon.[121]

An example of the latter is the Dense Inert Metal Explosive (DIME):

> DIME involves an explosive spray of superheated micro shrapnel made from milled and powdered Heavy Metal Tungsten Alloy (HMTA), which is highly lethal within a relatively small area. The HMTA powder turns to dust (involving even more minute particles) on impact. It loses inertia very quickly due to air resistance, burning and destroying through a very precise angulation everything within a four-meter range – and it is claimed to be highly carcinogenic and an environmental toxin. This new weapon was developed originally by the US Air Force and is designed to reduce collateral damage in urban warfare by limiting the range of explosive force.[122]

The 'capacity [of DIME] to cause untreatable and unnecessary suffering (particularly because no shrapnel is large enough to be readily detected or removed by medical personnel) has alarmed medical experts'.[123] The other concern with nanotechnology is that elements and chemicals that on a macro scale are not directly harmful to humans can be highly chemically reactive on the nanoscale. This may require a review of what international humanitarian law considers as chemical weapons.

Similarly, with the current advances in the understanding of the human genome and in neuroscience, there exists the very real possibility of militarization of this knowledge.[124] One of the legal consequences is a need to reappraise maintaining

120 J. Kellenberger, above note 15; ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, above note 29, p. 37.

121 H. Nasu and T. Faunce, above note 10, p. 23.

122 Whether such a weapon has been used in actual combat appears to remain a matter of speculation – see generally *Dense Inert Metal Explosive (DIME)*, Global Security, available at: http://www.globalsecurity.org/military/systems/munitions/dime.htm (last visited 8 May 2012).

123 H. Nasu and T. Faunce, above note 10, p. 22. Along with Art. 35(2) of API, above note 1, on unnecessary suffering, there is also *Protocol I of the Convention on Certain Conventional Weapons on Non-Detectable Fragments*, (10 October 1980). Amnesty International is of the view that 'further studies are required before it can be determined whether the use of DIME munitions is lawful under international law'. Amnesty International, 'Dense Inert Metal Explosives (DIME)', in *Fuelling conflict: foreign arms supplies to Israel/Gaza*, 2009, available at: http://www.amnesty.org/en/library/asset/MDE15/012/2009/en/5be86fc2-994e-4eeb-a6e8-3ddf68c28b31/mde150122009en.html#0.12. (last visited 8 May 2012). For a discussion generally of the *Protocol I of the Convention on Certain Conventional Weapons on Non-Detectable Fragments*, see W. Boothby, above note 45, pp. 196–199.

124 See generally Mark Wheelis and Malcolm Dando, 'Neurobiology: a case study for the imminent militarization of biology', in *International Review of the Red Cross*, Vol. 87, No. 859, 2005, p. 553. See also

a legal distinction between chemical and biological weapons. It may be that based on the manner in which they can be used we should legally view these weapons as part of a 'continuous biochemical threat spectrum, with the Chemical Weapons Convention and Biological and Toxin Weapons Convention (CWC and BTWC) overlapping in their coverage of mid-spectrum agents such as toxins and bioregulators'.[125]

There are competing tensions in this area. Quite understandably, chemical and biological weapons have a 'bad name'. At the same time, research is underway into non-lethal weapons such as incapacitating biochemical weapons.

> Although there is currently no universally agreed definition, incapacitating biochemical agents can be described as substances whose chemical action on specific biochemical processes and physiological systems, especially those affecting the higher regulatory activity of the central nervous system, produce a disabling condition (e.g., can cause incapacitation or disorientation, incoherence, hallucination, sedation, loss of consciousness). They are also called chemical incapacitating agents, biotechnical agents, calmatives, and immobilizing agents.[126]

A key point to note is that while traditional biological and chemical agents were used against enemy soldiers or non-cooperative civilians, and clearly would be classified as weapons, modern agents may be used to 'enhance' the capability of a state's own military forces. In such cases, it is much less likely that the agents would amount to weapons.[127] For example:

> within a few decades we will have performance enhancement of troops which will almost certainly be produced by the use of diverse pharmaceutical compounds, and will extend to a range of physiological systems well beyond the sleep cycle. Reduction of fear and pain, and increase of aggression, hostility, physical capabilities and alertness could significantly enhance soldier performance, but might markedly increase the frequency of violations of humanitarian law. For example, increasing a person's aggressiveness and hostility in conflict situations is hardly likely to enhance restraint and respect for legal prohibitions on violence.[128]

Similar concerns have already been expressed about remotely operated weapons. And in a manner similar to using directed energy weapons to disperse civilian

'Brain waves 3: neuroscience, conflict and security', in *The Royal Society*, available at: http://royalsociety.org/policy/projects/brain-waves/conflict-security (last visited 6 May 2012) for a discussion of, among other things, potential military applications of neuroscience and neurotechnology and current legal issues.

125 M. Wheelis and M. Dando, *ibid.*, p. 560.

126 Michael Crowley and Malcolm Dando, 'Submission by Bradford Nonlethal Weapons Research Project to Foreign Affairs Select Committee Inquiry on Global Security: Non-Proliferation', 2008, pp. 1–2, available at: http://www.brad.ac.uk/acad/nlw/publications/BNLWRP_FAC071108MC.pdf (last visited 8 May 2012).

127 Body armour, for example, is not classified as a weapon.

128 M. Wheelis and M. Dando, above note 124, pp. 562–563.

crowds, there is also the potential to pacify civilians in occupied territories through chemicals included in food distributions.[129] Perhaps of even more concern, as it goes directly to the ability to enforce international humanitarian law, particularly command responsibility, is the possibility of 'memories of atrocities committed [being] chemically erased in after-action briefings'.[130]

The need to understand the role of engineering in the weapon review process

The above overview of emerging weapons highlights that as weapons become more complex the ability for non-experts to understand the complex manner in which the weapon operates becomes increasingly difficult. This part of the article focuses on engineering issues and how an understanding of those issues can be factored into the legal review of weapons.

Why a weapon may not perform as intended

A weapon may not perform as intended or in accordance with the 'product design specification'[131] for a variety of reasons. Those reasons include: inadequate technical specification, design flaws, or poor manufacturing quality control (batch variation). Other factors include 'age of the munition, storage conditions, environmental conditions during employment, and terrain conditions'.[132]

A simple example of specification failure, or at least a specification that will not be 100 per cent reliable, is an anti-vehicle mine that is not intended to explode when stepped on by a human. For example, if it is a load activated mine, the load might be set to 150 kg. However, biomechanical research:

> shows very strong evidence that a human being can very easily exert an equivalent force close to and above such pressures. For example, an 8-year-old boy weighing 30 kg, running downhill in his shoes, exerts a ground force of 146 kg. A 9-year-old girl weighing 40 kg running downhill in her bare feet exerts 167 kg of force. An adult male running will exert 213 kg.[133]

Alternatively, the specification might be correct but the design, manufacturing process, or integration of systems does not consistently lead to the intended result. This may be an engineering quality issue where the implemented engineering

129 *Ibid.*, p. 565.
130 *Ibid.*, p. 565
131 The product design specification is a step before the actual technical specifications for a product. The former is about what a product should do, while the latter is concerned with how the product will do it.
132 *Defense Science Board Task Force, Munitions System Reliability*, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, US Department of Defense, Washington, DC, September 2005, p. 15, available at: http://purl.access.gpo.gov/GPO/LPS72288 (last visited 8 May 2012).
133 'Anti-vehicle mines: discussion Paper', Actiongroup Landmine.de, 2004, p. 5. (footnote omitted), available at: http://www.landmine.de/fileadmin/user_upload/pdf/Publi/AV-mines-discussion-paper.pdf (last visited 8 May 2012).

processes were inadequately robust leading to product flaws, and as such presents a reliability issue.

Where a weapon does not perform as intended, two prime consequences are:

- The desired combat effect is not achieved. If the weapon fails to perform, own forces are put at risk. If the weapon does not perform to specification, civilians and civilian property are put at risk.[134]
- Where civilians are injured or killed or civilian property damaged, liability may be incurred.[135] State liability may be incurred for an internationally wrongful act (i.e., a breach of the international humanitarian law) and criminal liability potentially attaches to the commander who authorized the use, or to the person who employed the weapon, or both.

As weapons systems become more complex, an understanding of reliability analysis will need to become part of the legal review process.

Reliability: test and evaluation

The purpose of test and evaluation is to provide an objective measurement of whether a system (or a component thereof) performs reliably to a specification. Reliability is the probability of correct functioning to a specified life (measured in time, cycles of operation, etcetera) at a given confidence level. Understanding that reliability is a key factor in weapon performance is intuitively simple but in fact has a level of complexity not always immediately grasped by those unfamiliar with reliability engineering.[136] Quantifying reliability is not a 'yes' or 'no' proposition,[137] nor can it be achieved by a single pass/fail test, but rather 'is subject to statistical confidence bounds'.[138] For example, to obtain an appropriate level of statistical confidence that the failure rate for a given weapon population is acceptable there are a minimum number of tests required. But as resources are always finite the question for responsible engineering practice is how to optimize resources and understand the minimum required resources to assure acceptable reliability? Suppose that undertaking the required number of tests will be too time-consuming or beyond budget allocation. A naïve approach would simply reduce the number of tests to meet budget requirements and presume that the test will still give some useful information. But that may not be the case. Arguably, the compromised test can only provide misleading conclusions if the result does not achieve the required level of confidence. For certification purposes, either a certain level of confidence is required or not. While the statistical confidence level may be set appropriately low

134 This has direct military effectiveness consequences, as well as effecting morale, domestic public support, international support, etcetera.

135 Liability may also arise where the means or method of warfare against combatants is unlawful, which may be the case in a defective weapon scenario, for example, firing on a combatant who is *hors de combat*.

136 See generally, *Defense Science Board Task Force on Munitions System Reliability*, above note 132.

137 'Just tell me whether it is reliable or not?' asks the hypothetical boss.

138 *Defense Science Board Task Force on Munitions System Reliability*, above note 132, p. 15.

for non-lethal weapon components where a failure has a low-operational impact and minor to no safety implications (e.g., failure of a tracer bullet), the target recognition system on an autonomous weapon may require a very high statistical confidence to minimize lethal weapon deployment on civilians while still ensuring engagement of enemy targets. If a high statistical assurance is deemed necessary for civilian safety while budgetary constraints preclude the corresponding necessary development testing, then appropriate limits should be implemented regarding the approved applications for that weapon until field experience provides appropriate reliability confidence.

How should this be applied in practice? The main steps of weapon acquisition are usefully outlined by McClelland, including the various testing stages during 'demonstration', 'manufacture', and 'in-service'.[139] As McClelland notes, this is not a legal process but rather part of the acquisition process; but nonetheless these steps provide decision points that are 'important stages for the input of formal legal advice'.[140] For testing to be meaningful, critical issues of performance must be translated into testable elements that can be objectively measured. While many smaller nations might be little more than purchasers of off-the-shelf weapons,[141] other governments are involved in envisaging, developing, and testing emerging weapons technology. While the degree of that involvement will vary, that is a choice for governments.[142] So, rather than being passive recipients of test results and other weapons data, one pro-active step that could be taken as part of the legal review process is for lawyers to input into the test and evaluation phases by identifying areas of legal concern that could then be translated into testable elements. This may be one way to at least partly address the security and compartmented access difficulties associated with high-technology weapons that were raised above. For example, it is appropriate to assign increased confidence in reliability for military applications involving higher risks factors for civilians. This could be cross-referenced against existing weapons system reliability data as an input to the decision-making process when determining whether a new targeting procedure may be considered lawful.

To be effective, the legal requirements need to be expressed in terms that are 'testable, quantifiable, measurable, and reasonable'.[143] Part of the challenge will

139 J. McClelland, above note 1, p. 401. Or during design, during initial acceptance, and as part of operational evaluation.

140 *Ibid.*, p. 402.

141 Of course, purchasers of off-the-shelf weapon systems must still satisfy themselves of the legality of a weapon. Even with a fully developed and tested weapon, this can still prove difficult for purchasers of high-technology weapons. For example, a manufacturer may refuse to disclose sufficient information about a high-technology weapon that uses encrypted proprietary software for the end-user to make an informed judgement about the algorithms used to be confident of the weapon's ultimate reliability.

142 See *Report on the Defense Science Board Task Force on Developmental Test & Evaluation*, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, US Department of Defense, May 2008, pp. 6–7, available at: www.acq.osd.mil/dsb/reports/ADA482504.pdf; wherein the recent decrease in US government involvement in design testing was highlighted, and perhaps more worryingly, government access to the contractor's test data was limited.

143 *Ibid.*, p. 38. Noting that this might initially be challenging. For example, *ibid.*, p. 39, for a discussion of where this has not occurred for the operational requirements.

be bridging the disconnect that often exists between the definitions of technical requirements and the desired operational performance. This disconnect can often be 'traced to the terminology used to define the level of performance required, under what conditions and how it is [to be] measured'.[144] This is where lawyers working with systems engineers can influence the process so that the use of tests, demonstrations, and analysis can be adopted as valid methods to predict actual performance.

Once a system is in-service, further testing may also be conducted to gain additional insights into the capability and to ensure that the system is actually meeting the requirements of the user. This phase of test and evaluation is particularly critical as it is the only phase that truly relates to the 'real world' use of a system.[145] By having lawyers provide meaningful legal criteria against which a class of weapons could be judged, the ongoing legal compliance of that weapon could be factored into an already existing process. Another area for useful input is evaluation and analysis of system and subsystem integration and interaction. When it comes to a system-of-systems, US military experience is that there is no 'single program manager who "owns" the performance or the verification responsibility across the multiple constituent systems, and there is no widely used adjudication process to readily assign responsibility for [system-of-systems] capabilities, with the exception of command and control systems'.[146] Compare this to other industries such as leading automotive companies that have highly sophisticated design, production, testing, and quality-approval processes for every component that goes into a vehicle and a resulting detailed assignment of responsibility by component, system, and whole product (comprising multiple systems). Working with systems engineers, layers of quality control process could identify the critical legal issues that require both testing and assignment of responsibility (for example, in case of non-compliance with international humanitarian law) among the weapon manufacturer and the various military stakeholders.

Reliability and automatic target recognition

Weapons that are designed to explode but fail to when used operationally, and if left on the field after the cessation of hostilities, are known as explosive remnants of war.[147] Indeed, munition reliability is even defined as 'a measure of the probability of successful detonation'.[148] Due to the effects on the civilian population of unexploded ordnance, legal regulation already exists in this area.[149] Less well

144 *Ibid.*, p. 41.

145 For example, there is anecdotal evidence that some weapon failures arise due to 'operational factors that are not assessed as part of the developmental, acceptance and surveillance testing', *Defense Science Board Task Force on Munitions System Reliability*, above note 132, p. 17.

146 *Report on the Defense Science Board Task Force on Developmental Test & Evaluation*, above note 142, p. 43.

147 See *Defense Science Board Task Force on Munitions System Reliability*, above note 132, p. 10.

148 *Ibid.*, p. 14.

149 For example, see the chapter on 'Unexploded and abandoned weapons', in W. Boothby, above note 45, pp. 297–317.

understood is that weapons reliability associated with automatic target recognition has another important aspect. It is not just about a weapon that does not explode, but also about one that selects the wrong target.

Here we are trying to determine whether it is reasonable to conclude from the analysis of reconnaissance data that the target possesses certain enemy properties or characteristics, and when is it reasonable to reach such a conclusion. Suppose the difference between the hypothesized enemy characteristic and the reconnaissance measurements is neither so large that we automatically reject the target, nor so small that we readily accept it. In such a case, a more sophisticated statistical analysis, such as hypotheses testing, may be required. Suppose that experience indicates that a 90 per cent match in reconnaissance data with existing information regarding an enemy target type has proven to be a reliable criterion for confirming an enemy target. If the data was a 100 per cent match or a 30 per cent match we could possibly come to an acceptable conclusion using common sense. Now suppose that the data match was 81 per cent, which may be considered relatively close to 90 per cent, but is it close enough to accept as a lawful target? Whether we accept or reject the data as a lawful target, we cannot be absolutely certain of our decision and we have to deal with uncertainty. The higher we set our data-match acceptance criterion the less likely an automatic target recognition system will identify non-targets as lawful targets, but the more probable that the recognition system will fail to identify lawful targets as being lawful targets.[150]

The desired level for whether or not a weapon explodes might be a 'reliable functioning rate of 95 per cent'.[151] This corresponds to an autonomous weapon system that fires at an unlawful target, due to misclassification as 'lawful', one out of every twenty times. Would this be considered acceptable performance for discriminating between lawful and protected targets? So, when a weapon system is looked at in this way, the better definition for reliability is whether the weapon system 'performs its intended function'[152] and as the 'fuzing and guidance capabilities become more integrated, the reliability of target acquisition must be measured and assessed'.[153] It has been suggested that what is required is a 'very high probability of correct target identification . . . and a very low probability of friendly or civilian targets being incorrectly identified as valid (i.e., enemy) targets'.[154] As there is an inherent trade-off between sensitivity and specificity, consideration also needs to be given to how a weapon will be employed. If a human provides go/no-go authorization based on an independent review, therefore providing additional safeguard against false recognition, then a greater number of false positives generated by the automatic recognition system may be acceptable. However, if the weapon system is autonomous, combat effect (correct employment against

150 See *Defense Science Board Task Force on Munitions System Reliability*, above note 132, p. 28.
151 *Ibid.*, p. 11. Even this level of reliability is based on controlled conditions and a lower level is allowed in operational conditions to account for 'environmental factors such as terrain and weather', *ibid.*, Appendix III, *DoD Policy Memo on Submunition Reliability*, p. 1.
152 *Ibid.*, p. 14.
153 *Ibid.*, p. 16.
154 *Ibid.*, p. 23.

identified enemy targets) must be more carefully balanced against risk to civilians. Noting that one of the purposes of automated and autonomous systems is to undertake high-volume observations that would overwhelm a human operator, where 'observations [are] in the millions . . . even very-low-probability failures could result in regrettable fratricide incidents'.[155] Confidence in the ability of an autonomous system to work in the real world might be developed by deploying such systems in a semi-autonomous mode where a human operator has to give the final approval for weapons release.[156] Rigorous post-mission analysis of data would allow, with time, a statistically significant assessment of the reliability of the system to correctly identify lawful targets.

A final point on testing:

> Achieving these gains [capability increases, manpower efficiencies, and cost reductions available through far greater use of autonomous systems] will depend on development of entirely new methods for enabling 'trust in autonomy' through verification and validation (V&V) of the near-infinite state systems that result from high levels of adaptability and autonomy. In effect, the number of possible input states that such systems can be presented with is so large that not only is it impossible to test all of them directly, it is not even possible to test more than an insignificantly small fraction of them. Development of such systems is thus inherently unverifiable by today's methods, and as a result their operation in all but comparatively trivial applications is uncertifiable.
>
> It is possible to develop systems having high levels of autonomy, but it is the lack of suitable V&V methods that prevents all but relatively low levels of autonomy from being certified for use. Potential adversaries, however, may be willing to field systems with far higher levels of autonomy without any need for certifiable V&V, and could gain significant capability advantages over the Air Force by doing so. Countering this asymmetric advantage will require as-yet undeveloped methods for achieving certifiably reliable V&V.[157]

A distinctly separate consideration from weapons testing is weapons research. Should weapons research (as opposed to development) be limited or constrained by legal issues? Generally, there is no legal reason (budgets aside) why research cannot take potential weapons as far as the bounds of science and engineering will allow, not the least of which is because laws change.[158] The time for imposing limits based on law is in the production and employment of weapons. Of course, some may, and

155 See *Report of Defense Science Board Task Force on Patriot System Performance: Report Summary*, above note 60, p. 2.

156 See A. Myers, above note 23, pp. 91–92.

157 US Air Force, 'Technology horizons', available at: http://www.af.mil/information/technologyhorizons.asp (last visited 6 May 2012).

158 See the examples of submarines and airplanes referred to in Anderson and Waxman, above note 29, pp. 6–7. While some aspects of international humanitarian law may change, this presumably does not extend to the cardinal principles of distinction, proportionality, and unnecessary suffering.

do, argue differently on moral and ethical lines.[159] That is where such arguments are best made and debated.

Conclusion

With the ever-increasing technological complexity of weapons and weapon systems, it is important that, among others, computer scientists, engineers, and lawyers engage with one another whenever a state conducts a review of weapons pursuant to Article 36 of the Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (API).[160] The reviews cannot be compartmentalized, with each discipline looking in isolation at their own technical area. Rather, those conducting legal reviews will require 'a technical understanding of the reliability and accuracy of the weapon',[161] as well as how it will be operationally employed.[162] While that does not mean lawyers, engineers, computer science experts, and operators need to each be multidisciplined, it does mean that each must have enough understanding of the other fields to appreciate potential interactions, facilitate meaningful discussion, and understand their own decisions in the context of impacts on other areas of development.

Those who develop weapons need to be aware of the key international humanitarian law principles that apply to the employment of weapons. Lawyers providing the legal input into the review of weapons need to be particularly aware of how a weapon will be operationally employed and use this knowledge to help formulate meaningful operational guidelines in light of any technological issues identified with the weapon in terms of international humanitarian law. Furthermore, all parties require an understanding of how test and validation methods, including measures of reliability, need to be developed and interpreted, not just in the context of operational outcomes, but also in compliance with international humanitarian law.

As the details of a weapon's capability are often highly classified and compartmentalized, lawyers, engineers, and operators may need to work co-operatively and imaginatively to overcome security classification and compartmental access limitations. One approach might be to develop clearly expressed legal

159 See Matthew Bolton, Thomas Nash and Richard Moyes, 'Ban autonomous armed robots', Article 36, 5 March 2012, available at: http://www.article36.org/statements/ban-autonomous-armed-robots/ (last visited 6 May 2012): 'Whilst an expanded role for robots in conflict looks unstoppable, we need to draw a red line at fully autonomous targeting. A first step in this may be to recognize that such a red line needs to be drawn effectively across the board – from the simple technologies of anti-vehicle landmines (still not prohibited) across to the most complex systems under development. This is not to ignore challenges to such a position – for example, consideration might need to be given to how automation functions in missile defence and similar contexts – but certain fundamentals seem strong. Decisions to kill and injure should not be made by machines and, even if at times it will be imperfect, the distinction between military and civilian is a determination for human beings to make'.

160 See P. Spoerri, above note 54.

161 K. Lawand, above note 1, pp. 929.

162 ICRC, *A Guide to the Legal Review of New, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*, above note 1, pp. 17–18.

parameters that can be the subject of meaningful systems testing. Another approach may be to devise multi-parameter acceptance criterion equation sets. Such equation sets would allow for hypothesis testing while factoring in reliability data, confidence levels, and risk factors using input data such as anticipated military advantage, weapon reliability data, reconnaissance measurement uncertainty, and civilian risk factors.

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

Cyber conflict and international humanitarian law

Herbert Lin

Dr Herbert Lin is Chief Scientist at the Computer Science and Telecommunications Board of the National Research Council (NRC), where he has also been Study Director of major projects on public policy and information technology. He was co-editor of the NRC's 2009 report *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*,[1] and a 2010 NRC study on cyber deterrence, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.*

Abstract

Conflict in cyberspace refers to actions taken by parties to a conflict to gain advantage over their adversaries in cyberspace by using various technological tools and people-based techniques. In principle, advantages can be obtained by damaging, destroying, disabling, or usurping an adversary's computer systems ('cyber attack') or by obtaining information that the adversary would prefer to keep secret ('cyber espionage' or 'cyber exploitation'). A variety of actors have access to these tools and techniques, including nation-states, individuals, organized crime groups, and terrorist groups, and there is a wide variety of motivations for conducting cyber attacks and/or cyber espionage, including financial, military, political, and personal. Conflict in cyberspace is different from conflict in physical space in many dimensions, and attributing hostile cyber operations to a responsible party can be difficult. The problems of defending against and deterring hostile cyber operations remain intellectually unresolved. The UN Charter and the Geneva Conventions are relevant to cyber operations, but the specifics of such relevance are today unclear because cyberspace is new compared to these instruments.

doi:10.1017/S1816383112000811

Keywords: cyber conflict, cyberspace, cyber attack, national security, international humanitarian law.

In the twenty-first century, information is the key coin of the realm, and thus entities, from nation-states to individuals are increasingly dependent on information and information technology (IT), including both computer and communications technologies. Businesses rely on information technology to conduct operations (such as payroll and accounting, recording inventory and sales, and research and development (R&D)). Distribution networks for food, water, and energy rely on IT at every stage, as do transportation, health care, and financial services. Factories use computer-controlled machinery to manufacture products more rapidly and more efficiently than ever before.

Military forces are no exception. IT is used to manage military forces – for example, for command and control and for logistics. In addition, modern precision-guided munitions illustrate how the use of IT embedded in weapons systems increases their lethality and reduces the collateral damage associated with the use of such weapons. Movements and actions of military forces can be coordinated through networks that allow information and common pictures of the battlefield to be shared widely.

Terrorists and other non-state armed groups also use IT. Although the kinetic weapons of terrorists are generally low-tech, terrorist use of IT for recruitment, training, and communications is often highly sophisticated.

A common term for networked information technology is 'cyberspace'. The US Department of Defense defines cyberspace as a domain characterized by 'the use of electronics [that is, IT] and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures'.[2] Using this definition, civilian, military, and terrorist entities operate in cyberspace to conduct their business and operations.

As noted in the writer's biography, the writer of this article is a US scientist and a policy analyst rather than a lawyer, but it is important to be aware that a full understanding of the cyber domain requires insight into technology, policy, and the law. Further, the analysis presented in this article generally reflects US perspectives on the issues discussed.

This article begins with a short primer on the nature of conflict in cyberspace, describing the tools and techniques of such conflict, the hostile (offensive) operations in cyberspace made possible by such tools and techniques, the actors that might use these tools and techniques, and the reasons why they might

1 The intellectual content of this report is drawn primarily from National Research Council (NRC), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, William Owens, Kenneth Dam, Herbert Lin (eds.), National Academies Press, Washington, DC, 2009, available at: http://www.nap.edu/catalog.php?record_id=12651. All internet references were accessed in August 2012, unless otherwise stated.

2 Department of Defense, '2006 National Military Strategy for Cyberspace Operations', available at: http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf.

do so. The second section addresses three important issues about conflict in cyberspace: comparing conflict in cyberspace to conflict in physical space using traditional kinetic weapons, attributing hostile operations to a responsible party, and defending against and deterring hostile operations. The third section addresses a number of important international legal issues relating to the UN Charter and the Geneva Conventions; it also addresses some of the potential human rights implications of offensive operations in cyberspace. The fourth section comments on the role of the private sector as both a target, and a conductor of offensive operations in cyberspace. The final section addresses the largely unexplored topics of preventing conflict escalation and terminating conflicts in cyberspace.

Perhaps the most important point of this paper is that it seeks to identify important questions associated with conflict in cyberspace, especially with respect to the international legal regime that governs such conflict. Alas, it cannot provide many answers to these questions – indeed, the need to develop new knowledge and insight into technical and legal instruments to support informed policy-making in this area will provide full employment for many analysts for a long time to come.

What is conflict in cyberspace?

Given the increasing importance of information and IT, it is not surprising that parties to a conflict might seek to gain advantage over their adversaries by using various tools and techniques for exploiting certain aspects of cyberspace – what this paper will call 'conflict in cyberspace' or 'cyber conflict'.[3]

Tools and techniques

The tools and techniques of conflict in cyberspace can be usefully separated into tools based on technology and techniques that focus on the human being. Offensive tools and techniques allow a hostile party to do something undesirable. Defensive tools and techniques seek to prevent a hostile party from doing so.

Technology-based tools

An offensive tool requires three components:

1. *Access* refers to how the hostile party gets at the IT of interest. Access may be remote (such as through the Internet, through a dial-up modem attached to it, or through penetration of the wireless network to which it is connected). Alternatively, access may require close physical proximity (for example, spies acting or serving as operators, service technicians, or vendors). Close access is also a possibility anywhere in the supply chain (for example, during chip

3 This definition implies that 'armed conflict' or 'military conflict' are subsets – and only subsets – of the broader term 'conflict', which may entail a conflict over economic, cultural, diplomatic, and other interests as well as conflict involving military matters or the use of arms.

fabrication, assembly, loading of system software, shipping to the customer, or operation).
2. A *vulnerability* is an aspect of the IT that can be used to compromise it. Vulnerabilities may be accidentally introduced through a design or implementation flaw, or introduced intentionally (see close access, above). An unintentionally introduced defect (or 'bug') may open the door for opportunistic use of the vulnerability by an adversary.
3. *Payload* is the term used to describe the mechanism for affecting the IT after access has been used to take advantage of a vulnerability. For example, once a software agent (such as a virus) has entered a computer, its payload can be programmed to do many things – reproducing and retransmitting itself, or destroying or altering files on the system. Payloads can be designed to do more than one thing, or to act at different times. If a communications channel is available, payloads can be remotely updated.

Defensive tools address one or more of these elements. Some tools (such as firewalls) close off routes of access that might be inadvertently left open. Other tools identify programming errors (vulnerabilities) that can be fixed before a hostile party can use them. Still others serve to prevent a hostile party from causing damage with any given payload (for example, a confidential file may be encrypted so that even if a copy is stolen from the system, it is useless to the hostile party).

People-based techniques

People interact with IT, and it is often easier to trick, bribe, or blackmail an insider into doing the bidding of a hostile party than it is to gain access through purely technological means. For example, close access to a system may be obtained by bribing a janitor to insert a USB flash drive into a computer. A vulnerability may be installed by blackmailing a programmer into writing defective code. Note that in such cases, technical tools and people-based techniques can be combined.

Defensive people-based techniques essentially involve inducing people not to behave in ways that compromise security. Education teaches (some) people not to fall for scams that are intended to obtain log-in names and passwords. Audits of activity persuade (some) people not to use IT in ways that are suspicious. Rewards for reporting persuade (some) people to report questionable or suspicious activity to the proper authorities.

Possible offensive operations in cyberspace

Offensive activity in cyberspace can be described as cyber attack or cyber exploitation.

- Cyber attack refers to the use of deliberate activities to alter, disrupt, deceive, degrade, or destroy computer systems or networks used by an adversary or the information and/or programs resident in or transiting through these systems or networks. The activities may also affect entities connected to these systems

and networks. A cyber attack might be conducted to prevent authorized users from accessing a computer or information service (a denial of service attack), to destroy computer-controlled machinery (the alleged purpose of the Stuxnet cyber attack[4]), or to destroy or alter critical data (such as timetables for the deployment of military logistics). Note that the direct effects of a cyber attack (damage to a computer) may be less significant than the indirect effects (damage to a system connected to the computer).

- Cyber exploitation refers to deliberate activities designed to penetrate computer systems or networks used by an adversary, for the purposes of obtaining information resident on or transiting through these systems or networks. Cyber exploitations do not seek to disturb the normal functioning of a computer system or network from the user's point of view – indeed, the best cyber exploitation is one that such a user never notices. The information sought is generally information that the adversary wishes not to be disclosed. A nation might conduct cyber exploitations to gather valuable intelligence information, just as it might deploy human spies to do so. It might seek information on an adversary's R&D program for producing nuclear weapons, or on the adversary's order of battle, its military operational plans, and so on. Or it might seek information from a company's network in another country in order to benefit a domestic competitor of that company. Of particular interest is information that will allow the country to conduct further penetrations on other systems and networks in order to gather additional information.

Note that press accounts often refer to 'cyber attacks' when the activity conducted is in fact a cyber exploitation.

Actors/participants and their motivations

What actors might conduct such operations? The nature of information technology is such that the range of actors who can conduct operations of national-level significance is potentially large. Certain nation-states, such as the United States, China, Russia, and Israel, are widely regarded as having potent offensive cyber capabilities, although less-developed nation-states can also conduct offensive operations in cyberspace.

To date, the known actors who have perpetrated acts of cyber exploitation and cyber attack are sub-national parties – mostly individuals, and mostly for profit. It is often alleged that Russia was behind the cyber attacks against Estonia in 2007 and Georgia in 2008,[5] that China is behind a number of high-profile cyber exploitations against entities in many nations,[6] and that the United States and/or Israel were responsible for the cyber attack on Iranian nuclear facilities (Stuxnet);

4 For a primer on Stuxnet, see 'Cyberattacks on Iran – Stuxnet and Flame', in *The New York Times*, 9 August 2012, available at: http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html?scp=1-spot&sq=stuxnet&st=cse.

5 See NRC, above note 1, box 3.4.

6 As this article goes to press, the American security firm Mandiant released on 19 February 2012, a detailed report concluding that a special unit of the Chinese People's Liberation Army is responsible for a large

however, none of these nations have officially acknowledged undertaking any of these activities, and conclusive proof, if any exists, that the political leadership of any nation ordered or directed any of these activities has not been made public.

A variety of sub-national actors – including individuals, organized crime groups, and terrorist groups – might conduct cyber attacks and/or cyber exploitations. Indeed, some (but only some) such operations can be conducted with information and software found on the Internet and hardware available at any local computer store.

Motivations for conducting such operations – that is, for engaging in cyber conflict – also span a wide range. One of the most common motivations today is financial. Because a great deal of commerce is enabled through the Internet or through the use of IT, some parties are cyber criminals who seek illicit financial gain through their offensive actions. Cyber exploitations can yield valuable information, such as credit card numbers or bank log-in credentials; trade secrets; business development plans; or contract negotiation strategies. Cyber attacks can disrupt the production schedules of competitors, destroy valuable data belonging to a competitor, or be used as a tool to extort money from a victim. Perpetrators might conduct a cyber attack for hire (it is widely believed that the cyber attack on Estonia was conducted using a rented cyber weapon).[7]

Another possible reason for such operations is political – the perpetrator might conduct the operation to advance some political purpose. A cyber attack or exploitation may be conducted to send a political message to a nation, to gather intelligence for national purposes, to persuade or influence another party to behave in a certain manner, or to dissuade another party from taking certain actions.

Still another reason for conducting such operations is personal – the perpetrator might conduct the operation to obtain 'bragging rights', to demonstrate mastery of certain technical skills, or to satisfy personal curiosities.

Lastly, such operations may be conducted for military reasons, in the same way that traditional military operations involving kinetic weapons are used.

Some important issues

Cyber conflict raises many complex issues for national security. The issues described below are presented as a sample of the most salient, but this overview is not intended to be comprehensive.

How conflict in cyberspace compares to conflict in physical space

Much about cyber conflict upends our understanding of how conflict might unfold. Although most observers would acknowledge clear differences between the cyber

fraction of the cyber intrusions conducted against American corporations, organizations, and government agencies. See http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

7 William Jackson, 'Cyberattacks in the present tense, Estonian says', in *Government Computing News*, 28 November 2007, available at http://www.gcn.com/online/vol1_no1/45476-1.html.

and physical domains, it is easy to underestimate just how far-reaching these differences are. Consider, for example, the impact of:

- Venue for conflict. In traditional kinetic conflict (TKC – that is, *conflict* conducted with kinetic weapons by organized, governmentally controlled forces), many military activities (specifically, those in the air and on or under the ocean) occur in a space that is largely separate from the space in which large numbers of civilians are found. In cyber conflict, the space in which many military activities occur is one in which civilians are ubiquitous.
- The offence-defence balance. In TKC, offensive technologies and defensive technologies are often in rough balance. In cyber conflict (at least prior to the outbreak of overt hostilities), the offence is inherently superior to the defence, in part because the offence needs to be successful only once, whereas the defence needs to succeed every time, and in part because there is no way to guarantee that harmful, incorrect, or flawed information inputs (either programs or data) will not be entered into an IT-based system.
- Attribution. TKC is conducted by military forces that are presumed to be under the control of national governments. No such presumptions govern the actors participating in cyber conflict, and definitive attribution of acts in cyberspace to national governments is very difficult or impossible (see discussion below).
- Capabilities of non-state actors. In TKC, the effects that are produced are generally a function of the number of military personnel that can engage in combat, and since such numbers tend to be smaller for non-state actors than those available to states, the effects that non-state actors can produce are relatively small compared to those that can be produced by comparably equipped state actors. In cyber conflict, non-state actors can leverage the capabilities of IT to produce some of the large-scale effects that can be achieved by large-scale actors.
- The importance of distance and national borders. In TKC, distance looms large, and violations of national borders are significant. In cyber conflict, distance is more or less irrelevant, and penetrations of national boundaries for both attack and exploitation occur routinely and without being noticed.

Attribution

As noted above, a key technical attribute of cyber operations is the difficulty of attributing any given cyber operation to its perpetrator. In this context, the definition of 'perpetrator' can have many meanings:

- The attacking machine that is directly connected to the target. Of course, this machine – the one most proximate to the target – may well belong to an innocent third party who has no knowledge of the operation being conducted.
- The machine that launched or initiated the operation.
- The geographical location of the machine that launched or initiated the operation.

- The individual sitting at the keyboard of the initiating machine.
- The nation under whose jurisdiction the named individual falls (for example, by virtue of his physical location when he typed the initiating commands). Thus, a machine located in Russia could be controlled by an individual in France acting at the behest of the Iranian government.
- The entity under whose auspices the individual acted, if any.

In practice, a judgement of attribution is based on all available sources of information, which could include technical signatures and forensics collected regarding the act in question, intelligence information (such as intercepted phone calls monitoring the conversations of senior leaders), prior history (similarity to previous cyber operations, for example), and knowledge of those with incentives to conduct such operations.

It is commonly said that attribution of hostile cyber operations is impossible. This statement does have an essential kernel of truth: if the perpetrator makes no mistakes, uses techniques that have never been seen before, leaves behind no clues that point to himself, does not discuss the operation in any public or monitored forum, and does not conduct his actions during a period in which his incentives to conduct such operations are known publicly, then identification of the perpetrator may well be impossible.

Indeed, sometimes all of these conditions are met, and policy-makers rightly despair of their ability to act appropriately under such circumstances. But in other cases the problem of attribution is not so dire, because one or more of these conditions are not met, and it may be possible to make some useful (if incomplete) judgements about attribution. For example, even if one does not know the location of the machine that launched a given attack, signals or human intelligence might provide the identity of the entity under whose auspices the attack was launched. The latter might be all that is necessary to take further action against the perpetrator.

Deterrence and defence in cyberspace

A great deal of policy attention today is given to protecting information and IT that is important to the nation. There are two ways (not mutually exclusive) of providing such protection: defending one's assets against offensive actions, and dissuading a hostile party from taking such actions.

Defence involves measures that decrease the likelihood that an offensive action will succeed. These include measures that prevent a perpetrator from gaining access, that eliminate vulnerabilities, or that enable the victim of an operation to recover quickly from a successful offensive action.

Dissuasion involves persuading an adversary not to launch the offensive action in the first place. Deterrence is an approach to dissuasion that involves the certain imposition of high costs on any adversary that is unwise enough to initiate an offensive action. Such costs may be imposed on an identified adversary in the cyber domain in response to some hostile action in cyberspace. There is no

logical need to restrict a response to this domain, however, and decision-makers have a wide choice of response options that include changes in defensive postures, law enforcement actions, economic actions, diplomacy, and military operations involving traditional forces, as well as cyber operations.

The United States' national security posture has traditionally been based on a robust mix of defence and deterrence, but cyberspace turns this mix on its head. The inherent superiority of offensive cyber operations over defensive operations has led many to consider a strategy of deterrence to dissuade adversaries from conducting such operations against the United States. But senior policy-makers have concluded that because deterrence in cyberspace is such a difficult strategy to implement, we must do a more effective job of defence.[8] If the reader finds this intellectual state of affairs unsatisfactory, he is not alone.

The laws of war as they apply to cyber conflict

The differences between TKC and cyber conflict have pervasive effects on how we should conceptualize conflict. The Law of Armed Conflict (LOAC) and the laws regulating the use of force in international relations found in the UN Charter were developed to cope with TKC, but although the fundamental principles underlying these laws remain valid, how they apply to cyber conflict in any specific instance is at best uncertain today. The intuitions of commanders (and their legal advisers) have been honed in environments of TKC. And apart from a few specialists, an understanding of cyber conflict does not exist broadly within the personnel of today's armed forces.

Armed conflict between nations (or 'international armed conflict') is today governed by two bodies of international law: *jus ad bellum*, the body of law that governs the question when a nation may have recourse to armed force (any such recourse between states amounting to an 'armed conflict'), and *jus in bello*, the body of law that regulates how a party engaged in an armed conflict must behave. The sources of both bodies of law are listed in Article 38 of the Statute of the International Court of Justice (ICJ), and are to be found primarily in treaties (written agreements among nations) and customary international law (that is, rules that come from 'a general practice accepted as law' and that exist independent of treaty law).[9]

This section provides a short overview of the legal dimensions of cyber conflicts. Other articles in this publication address this topic in more detail.[10]

8 William Lynn, 'Defending a new domain: the Pentagon's cyberstrategy', in *Foreign Affairs*, Vol. 89, No. 5, September–October 2010, available at: http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

9 Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law, Volume I: Rules*, ICRC/Cambridge University Press, Cambridge, 2005, available at: http://www.icrc.org/eng/war-and-law/treaties-customary-law/customary-law/index.jsp.

10 See Cordula Droege, 'Get off my cloud – Cyber warfare, international humanitarian law and the protection of civilians' in this edition of the *Review*.

Jus ad bellum

Today, the primary treaty source of *jus ad bellum* is the United Nations Charter, which explicitly forbids all signatories from using force (Article 2(4)) except in two instances – when authorized by the Security Council (pursuant to a resolution issued under Chapter VII of the UN Charter), and when a signatory is exercising its inherent right of self-defence when it has been the target of an armed attack (pursuant to Article 51). Complications and uncertainty regarding how the UN Charter should be interpreted when cyber attacks occur result from three fundamental facts.

First, the UN Charter was written in 1945, long before the notion of cyber attacks was even imagined. The underlying experiential base for the formulation of the Charter involved TKC among nations, and thus the framers of the Charter could not have imagined how it might apply to cyber conflict.

Second, the UN Charter itself contains no definitions for certain key terms, such as 'use of force', 'threat of force', or 'armed attack'. Thus, what these terms mean cannot be understood by direct reference to the Charter. Definitions and meanings can only be inferred from historical precedent and practice – how individual nations, the United Nations itself, and international judicial bodies have defined these terms in particular instances. Given a lack of clarity for what these terms might mean in the context of TKC, it is not surprising that there is even less clarity for what they might mean in the context of cyber conflict. One might therefore hope for future case law to clarify those terms, as it did for TKC. How and even whether case law will hear about cases involving cyber attack is entirely unclear at this point, however.

Third, the Charter is in some ways internally inconsistent. Article 2(4) bans uses of force that could damage persons or property other than in self-defence or authorized by the UN Security Council. However, Article 41 allows other acts (specifically, economic sanctions) that could damage persons or property. The use of operations not contemplated by the framers of the UN Charter – that is, cyber operations – may well magnify such inconsistencies. An example will help to illustrate some of the complications that may arise. An offensive operation involving a number of cyber attacks conducted over time against a variety of different financial targets in an adversary nation could cause extensive economic loss and panic in the streets, and shake public confidence in the incumbent regime, but without directly causing physical damage or any loss of life. Assuming the perpetrator of this operation could be identified, on what basis, if any, would such an operation be construed under the UN Charter as a use of force or an armed attack, rather than as an economic or 'political' sanction?

One possible answer to this question – put simply, what would constitute an armed attack in cyberspace? – is that if a cyber attack causes the same effects as a kinetic attack that rises to the threshold of an armed attack, the cyber attack would itself be considered an armed attack.

The answers to such questions under various circumstances involving cyber attack matter both to the attacked party and the attacking party.

- The answers matter to the attacked party because they may influence when and under what governmental agency the response may occur (for example, in the United States, the answers influence whether the attack is considered a law enforcement or military matter), and what rights the victim might have in responding.
- The answers matter to the attacking party because they set a threshold for a legal recourse to force that policy-makers may not wish to cross in taking assertive/aggressive actions to further the party's interests.

Jus in bello

Jus in bello is based in large part on the provisions of the Geneva Conventions and their customary counterparts. Some of the fundamental principles underlying *jus in bello* are the principle of military necessity (military operations must be intended to assist in the military defeat of the enemy and must serve a concrete military purpose) the principle of distinction (military operations may be conducted only against 'military objectives' and not against civilian targets), and the principle of proportionality (the expected incidental loss of civilian life, injury to civilians or damage to civilian objects must not be disproportionate to the anticipated military advantage).

As with the UN Charter, the Geneva Conventions are silent on cyber attack as a modality of conflict, and the question of how to apply the principles mentioned above in any instance involving cyber conflict may be problematic. The following hypothetical cases are offered to raise some key issues:

- Under the provisions of the Geneva Conventions and Additional Protocols related to distinction, parties to a conflict must distinguish between civilians and combatants and between civilian objects and military targets.[11] In the context of cyber warfare, an attack on an adversary's IT system or network would have to be intended to result in a definite military advantage (and not merely a political or economic advantage).[12] Today, military forces are likely to route a large fraction of their communications over communications facilities that are primarily used for civilian purposes. Similarly, military bases often depend on the host nation's power grid. Do these facts suggest that communications facilities and power grids would be valid military targets?[13]

11 Additional Protocol I of 1977 (hereafter AP I), Art. 48; and see J.-M. Henckaerts and L. Doswald-Beck (eds), above note 9, rule 7.

12 AP I, Art. 52(2).

13 Communications facilities and power grids could be considered examples of dual-use entities. The legality of deliberately targeting dual-use entities is not explicitly addressed in the text of the Geneva Conventions or the Additional Protocols thereto. However, the ICRC Commentary of the Additional Protocols of 1977 (commentary of Art. 52(2)), para. 2023, suggests that attacks on such entities are permissible, although the proportionality test for an attack must be satisfied as well. Attacks on such entities conducted with

- The provisions related to precautions against the effects of attacks also require the party targeted in an attack to protect civilians and civilian objects under its control against the effects of attacks – for example, by not locating military targets within or near densely populated areas and by removing civilian persons and objects from the vicinity of military targets.[14]
- Under the provisions related to proportionality,[15] some degree of collateral damage is allowable, but not if the 'expected' collateral damage is disproportionate compared to the 'anticipated military advantage'.[16] If, for example, a power plant is the target of a cyber attack, an assessment must be made as to whether the harm to the civilian population caused by disruption of electrical service is not disproportionate to the military advantage that might ensue from attacking the plant. Before such an assessment could be made, the commander would have to have adequate intelligence about the plant (and what was dependent on the plant) on which to base the judgement.
- The provisions related to non-perfidy state that military forces cannot pretend to be legally protected entities, such as hospitals. The rule is a consequence of maintaining the distinction between civilian and military entities. What if nation A uses the information systems of a hospital as a launching point for its cyber attacks against nation B? Can a cyber counterattack legally be launched against the information systems involved?
- Another crucial issue relates to the status of the operator. In the case of international armed conflict, a civilian operator would benefit from immunity from attack unless he or she took a 'direct part in hostilities',[17] at which time he or she would become a legitimate military target. Given that civilians will likely be key participants in conducting certain kinds of cyber attacks, how and to what extent, if any, does the criterion of direct participation relate to the planning, preparation, and/or execution of a cyber attack? Consider, for example, the following spectrum of civilian involvement:
  - A civilian posts a vulnerability notice for the open-source Linux operating system that a cyber attack exploits.
  - A civilian contractor for the DOD identifies the presence of this vulnerability on an adversary's system.
  - A civilian contractor exploits the vulnerability by introducing a hostile agent into the adversary's system that does not damage it but that can be directed to cause damage at a subsequent time.
  - A civilian contractor dictates to a military officer the precise set of commands needed to activate the hostile agent.

the intention of injuring civilians or damaging civilian property would not be legitimate, but making that determination is difficult.

14 AP I, Art. 58. See also J.-M. Henckaerts and L. Doswald-Beck (eds), above note 9, rules 22–24.

15 As codified in AP I, Art. 51(5)(b) and Art. 57(2)(a)(iii); see also J.-M. Henckaerts and L. Doswald-Beck (eds), above note 9, rule 14.

16 AP I, Art. 51(5)(b).

17 AP I, Art. 51(3).

Such examples suggest that there may be considerable uncertainty about how a serious LOAC analysis of any given operational scenario might proceed if cyber attacks were involved.

Potential human rights implications

Human rights restrain governmental action with respect to individuals under the government's jurisdiction. Such rights can originate nationally (such as the rights granted to Americans under the United States Constitution), in international treaties (such as the Convention on the Elimination of All Forms of Discrimination Against Women), or in customary international law.

Two of the rights enumerated in the International Covenant on Civil and Political Rights (ratified by the United States in September 1992) may be relevant to the cyber domain. Article 17 (protecting privacy and reputation) might be relevant to cyber operations intended to harm the reputation of an individual – for example, by falsifying computer-based records about transactions in which he or she had engaged – or to uncover private information about an individual (potentially constituting a provocation prior to conflict if the individual is prominent or politically influential). Article 19 (protecting rights to seek information) might be relevant to cyber attacks intended to prevent individuals from obtaining service from the Internet or other media. A number of other rights, such as the rights to life, to health, and to food, may be implicated as well depending on the nature and targets of the cyber attack. Respect for these other rights could suggest, for example, that a cyber attack intended to enforce economic sanctions would still have to allow transactions related to the acquisition of food and medicine.

A number of nations have declared that access to the Internet is a fundamental right of their societies (as of August 2011, these nations include Estonia,[18] France,[19] Spain,[20] and Finland[21]). Thus, if access to the Internet is a human right, then actions curtailing or preventing Internet access violate that right.

In addition, an important and contested point in human rights law is the extent of its applicability during acknowledged armed conflict or hostilities. The position of the United States government is that the imperatives of minimizing unnecessary human suffering are met by the requirements of the LOAC, and thus that human rights law should not place additional constraints on the actions of its armed forces. By contrast, a number of international bodies, such as

18 Colin Woodard, 'Estonia, where being wired is a human right', in *The Christian Science Monitor*, 1 July 2003, available at: http://www.csmonitor.com/2003/0701/p07s01-woeu.html.

19 'Top French court declares internet access "basic human right"', in *FoxNews.com*, 12 June 2009, available at: http://www.foxnews.com/story/0,2933,525993,00.html.

20 'Spain govt to guarantee legal right to broadband', in *Reuters*, 17 November 2009, available at: http://www.reuters.com/article/2009/11/17/spain-telecoms-idUSLH61554320091117.

21 '1Mb Broadband access becomes legal right', in *Yle Uutiset*, 14 October 2009, available at: http://yle.fi/uutiset/1mb_broadband_access_becomes_legal_right/1080940.

the ICJ[22] and the Human Rights Committee,[23] argue that human rights law can and should apply as well as LOAC during hostilities.

The role of the private sector as target and conductor of offensive cyber operations

The private sector is deeply involved in matters related to cyber conflict in many ways – and much more so than it is involved in traditional kinetic conflict. The most obvious connection is that private-sector entities are quite often the targets of hostile cyber operations. The perpetrators of most such operations against private-sector entities are generally believed to be criminals (such as those seeking credit card numbers), but nation-states may conduct cyber operations against them for a variety of purposes as well (as discussed in the section 'Deterrence and defence in cyberspace', above).

In addition and especially in the United States, military and civilian actors share infrastructure to a very large degree. A very large fraction of US military communications pass over networks owned by the private sector and operated largely for the benefit of civilian users. The same is true for electric power – US military bases depend on the civilian power grid for day-to-day operations. Under many interpretations of the LOAC, military dependence on civilian infrastructure makes that civilian infrastructure a legitimate target (a 'dual-use object') for an adversary's military operations.

Another important connection is that the artefacts of cyberspace are largely developed, built, operated, and owned by private-sector entities or companies that provide IT-related goods and services. In some cases, the cooperation of these entities may be needed to provide adequate defensive measures. For example, some policy-makers argue that an adequate defensive posture in cyberspace will require the private sector to authenticate users in such a way that anonymous behaviour is no longer possible. In other cases, private-sector cooperation may be needed to enable offensive cyber operations against adversaries. For example, the cooperation of a friendly internet service provider may be needed to launch a cyber attack over the Internet.

Many questions arise regarding the private sector's connection to cyber conflict. For example:

- What actions beyond changes in defence posture and informing law enforcement authorities should the private sector be allowed to take in response

22 ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996, *ICJ Reports 1996*, para. 25; ICJ, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 9 July 2004, *ICJ Reports 2004*, paras. 106–113; ICJ, *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Judgement, 19 December 2005, *ICJ Reports 2005*, para. 216.

23 UN Human Rights Committee, General Comment No. 31, CCPR/C/21/Rev.1/Add.13, 26 May 2004, para. 11.

to hostile cyber operations? Specifically, how aggressive should the responses of private-sector entities be?
- How and to what extent, if any, should the United States government conduct offensive operations to respond to cyber attacks on private-sector entities (or authorize an aggressive private-sector response)? Under what circumstances, if any, should it do so?
- How might private-sector actions interfere with US government cyber operations?
- What is the United States government's responsibility for private-sector actions that rise to the threshold of 'use of force' (in the UN Charter sense of the term)?

Preventing escalation and terminating conflicts in cyberspace

Small conflicts can sometimes grow into larger ones. Of particular concern to decision-makers is the possibility that the violence could increase to a level not initially contemplated or desired by any party to the conflict.

In considering TKC, analysts have often thought about escalation dynamics and terminating conflict. In a cyber context, escalation dynamics refers to the possibility that initial conflict in cyberspace may grow. Much of the thinking regarding cyber conflict is focused on the first (initial) stages of conflict – it asks, for example, 'What do we do if X conducts a serious cyber attack on the United States?', with the implicit assumption that such a serious attack would be the first cyber attack.

But what if it is not? How would escalation unfold? How could it be prevented (or deterred)? There are theories of escalation dynamics, especially in the nuclear domain, but because of the profound differences between the nuclear and cyber domains, there is every reason to expect that a theory of escalation dynamics in cyberspace would be very different from a theory of escalation dynamics in the nuclear domain. Some of the significant differences include the fact that attribution is much slower and/or more uncertain, the fact that the ability of non-state actors to interfere in the management of a conflict is increased in cyber conflict, and the existence of a multitude of states that have meaningful capabilities to conduct cyber operations.

Escalation can occur through a number of mechanisms (which may or may not simultaneously be operative in any instance).[24] One party to a conflict may deliberately escalate the conflict with a specific purpose in mind. It might inadvertently escalate the conflict by taking an action that it does not believe is escalatory but that its opponent perceives as escalatory. It might accidentally escalate a conflict if its forces take some unintended action (such as striking the wrong target). Lastly, catalytic escalation occurs when some third party

24 RAND, *Dangerous Thresholds: Managing Escalation in the 21st Century*, 2008, available at: http://www.rand.org/pubs/monographs/2008/RAND_MG614.pdf.

succeeds in provoking two parties to engage in conflict ('let's you and him fight'). Catalytic provocation is facilitated by the possibility of anonymous or unattributable action.

Conflict termination in cyberspace poses many difficulties as well. Conflict termination is the task faced by decision-makers on both sides when they have agreed to cease hostilities. A key issue in implementing such agreements is knowing that the other side is abiding by the negotiated terms. How would one side know that the other side is honouring a cease-fire in cyberspace, given the risk that one or both sides are likely to be targets of hostile cyber operations from third parties independently from the cyber conflict between the two principal actors? In other words, there is a constant background of hostile cyber operations going on all the time. And would one side be obliged to inform the other of all of the battlefield preparations it had undertaken prior to the conflict? Such an act, analogous to de-mining operations, would require each side to keep careful track of its various preparations.

Conclusion

Conflict can and does occur in cyberspace. How and to what extent does recent history about conflict in cyberspace presage the future?

Two things are clear today. First, only a small fraction of the possibilities for cyber conflict has been experienced to date, and actual experience with cyber conflict has been limited. Indeed, nearly all of the adversarial actions known to have been taken in cyberspace against the United States or any other nation, including both cyber attack and cyber exploitation, have fallen short of any plausible threshold for defining them as 'armed conflict', 'use of force', or even 'armed attack'. This fact has two consequences: there are many possibilities for serious cyber conflict that have not yet been seen,[25] and the question of how to respond to hostile actions in cyberspace that do not rise to these thresholds is the most pressing concern of policy-makers today, as nearly all hostile cyber operations conducted to date do not rise to these thresholds.[26]

Second, many of our assumptions and understandings about conflict – developed in the context of TKC – either are not valid in cyberspace or are applicable only with difficulty. Thus, decision-makers are proceeding into largely unknown territory – a fact that decreases the predictability of the outcome of any actions they might take.

25 Gregory Rattray and Jason Healey, 'Categorizing and understanding offensive cyber capabilities and their use', in NRC, *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, National Academies Press, Washington, D.C., 2010, pp. 77–98, available at: http://www.nap.edu/catalog/12997.html.

26 Herbert Lin, 'Responding to sub-threshold cyber intrusions: a fertile topic for research and discussion', in *Georgetown Journal of International Affairs*, Special Issue, *International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity*, 2011, pp. 127–135.

The 2009 NRC report on which this article is based[27] recommended *inter alia* that the United States government conduct a broad, unclassified national debate about cyber attack policy, and that it should work to find common ground with other nations regarding cyber attack, where common ground included better mutual understanding regarding various national views of cyber attack, how the laws of war and the UN Charter might or might not apply to cyber attack, the significance of non-state parties that might launch cyber attacks, and how nations should respond to such attacks. Both of these recommendations[28] are still valid today, and indeed they constitute good advice not only for the United States government but also for the governments of all nations that are party to the UN Charter and the Geneva Conventions.

27 See NRC, above note 1.
28 See *Idem*., recommendations 2 and 3.

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians

Cordula Droege*

Cordula Droege is the Head of the Operational Law Unit, Legal Division, International Committee of the Red Cross (ICRC).

Abstract

Cyber warfare figures prominently on the agenda of policymakers and military leaders around the world. New units to ensure cyber security are created at various levels of government, including in the armed forces. But cyber operations in armed conflict situations could have potentially very serious consequences, in particular when their effect is not limited to the data of the targeted computer system or computer. Indeed, cyber operations are usually intended to have an effect in the 'real world'. For instance, by tampering with the supporting computer systems, one can manipulate an enemy's air traffic control systems, oil pipeline flow systems, or nuclear plants. The potential humanitarian impact of some cyber operations on the civilian population is enormous. It is therefore important to discuss the rules of international humanitarian law (IHL) that govern such operations because one of the main objectives of this body of law is to protect the civilian population from the effects of warfare. This article seeks to address some of the questions that arise when applying IHL – a body of law that was drafted with traditional kinetic warfare in mind – to cyber technology. The first question is: when is cyber war really war in the sense of

* I would like to thank my colleagues from the ICRC, Knut Dörmann, Bruno Demeyere, Raymond Smith, Tristan Ferraro, Jelena Pejic, and Gary Brown for their thoughtful comments on earlier drafts, as well as Nele Verlinden for her help with the references.
All the Internet references were accessed in October 2012, unless otherwise stated.
This article was written in a personal capacity and does not necessarily reflect the views of the ICRC.

doi:10.1017/S1816383113000246

'armed conflict'? After discussing this question, the article goes on to look at some of the most important rules of IHL governing the conduct of hostilities and the interpretation in the cyber realm of those rules, namely the principles of distinction, proportionality, and precaution. With respect to all of these rules, the cyber realm poses a number of questions that are still open. In particular, the interconnectedness of cyber space poses a challenge to the most fundamental premise of the rules on the conduct of hostilities, namely that civilian and military objects can and must be distinguished at all times. Thus, whether the traditional rules of IHL will provide sufficient protection to civilians from the effects of cyber warfare remains to be seen. Their interpretation will certainly need to take the specificities of cyber space into account. In the absence of better knowledge of the potential effects of cyber warfare, it cannot be excluded that more stringent rules might be necessary.

Keywords: cyber security, cyber warfare, cyber attack, international humanitarian law, cyber operations, cyber weapons, armed conflict in cyber space, conduct of hostilities, distinction, proportionality, indiscriminate attacks, precautions.

Introduction

Cyber security figures prominently on the agenda of policymakers and military leaders around the world. A recently published study by the United Nations Institute for Disarmament Research (UNIDIR) describes the measures taken by thirty-three states that have specifically included cyber warfare in their military planning and organisation, and gives an overview of the cyber security approach of thirty-six other states.[1] These range from states with very advanced statements of doctrine and military organisations employing hundreds or thousands of individuals to more basic arrangements that incorporate cyber attack and cyber warfare into existing capabilities for electronic warfare. A number of states are setting up specialized units in or outside of their armed forces to deal with cyber operations.[2] It has also been reported that twelve of the world's fifteen largest military forces are building cyber warfare programmes.[3]

Cyber security in general and cyber warfare in particular

Amid much discussion about cyber security generally, the public at large knows little, yet, of the military planning and policies of states for cyber warfare.

1 Center for Strategic and International Studies, *Cybersecurity and Cyberwarfare – Preliminary Assessment of National Doctrine and Organization*, UNIDIR Resources Paper, 2011, available at: http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf; see also, Eneken Tikk, *Frameworks for International Cyber Security*, CCD COE Publications, Tallinn, 2011.

2 See, e.g., Ellen Nakashima, 'Pentagon to boost cybersecurity force', in *The Washington Post*, 27 January 2013; Gordon Corera, 'Anti-cyber threat centre launched', in *BBC News*, 27 March 2013.

3 Scott Shane, 'Cyberwarfare emerges from shadows of public discussion by US officials', in *The New York Times*, 26 September 2012, p. A10.

It appears that most government strategies consist of a mix of defensive and offensive strategies. On the one hand, states are increasingly seeking to protect their own critical infrastructure from cyber attacks. On the other hand, they appear also to be building technological capacities to be able to launch cyber operations against their adversaries in times of armed conflict.[4]

Policymakers and commentators are debating whether all or some of the new 'cyber weapons' should be banned altogether, whether attention should turn to confidence-building measures (similar to those on nuclear disarmament),[5] or whether 'rules of the road' should be established for behaviour in cyber space.[6] There has also been discussion for over a decade about the need for a new treaty on cyber security. The Russian Federation has advocated for such a treaty since the late 1990s, whereas the United States of America (US) and Western states have taken the position that none is needed.[7] In a letter to the Secretary-General of the United Nations (UN), China, the Russian Federation, Tajikistan, and Uzbekistan proposed an International Information Security Code of Conduct in September 2011, but this has a much broader scope than just for situations of armed conflict.[8] China, the Russian Federation, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan are also parties to an agreement adopted in the framework of the Shanghai Cooperation Organisation in 2009.[9] India, the Islamic Republic of Iran, Mongolia, and Pakistan participate as observers. An unofficial English translation of this agreement shows that it appears to enlarge the concepts of 'war' and 'weapon' beyond their traditional meaning in international humanitarian law (IHL).[10]

4 *Ibid.*

5 Ben Baseley-Walker, 'Transparency and confidence-building measures in cyberspace: towards norms of behaviour', in UNIDIR, *Disarmament Forum,* 'Confronting cyberconflict', Issue 4, 2011, pp. 31–40, available at: http://www.unidir.org/files/publications/pdfs/confronting-cyberconflict-en-317.pdf; James Andrew Lewis, *Confidence-building and international agreement in cybersecurity*, available at: http://www.unidir.org/pdf/articles/pdf-art3168.pdf.

6 See William Hague, 'Security and freedom in the cyber age – seeking the rules of the road', Speech to the Munich Security Conference, 4 February 2011, available at: https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road, and 'Foreign Secretary opens the London Conference on Cyberspace', 1 November 2011, available at: https://www.gov.uk/government/speeches/foreign-secretary-opens-the-london-conference-on-cyberspace.

7 See draft resolution submitted by the Russian Federation to the General Assembly First Committee in 1998, letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations Secretary-General, UN Doc. A/C.1/53/3, 30 September 1998; John Markoff and Andrew E. Kramer, 'US and Russia differ on a treaty for cyberspace', in *The New York Times*, 28 June 2009, p. A1; John Markoff and Andrew E. Kramer, 'In shift, US talks to Russia on internet security', in *The New York Times*, 13 December 2009, p. A1; see Adrian Croft, 'Russia says many states arming for cyber warfare', in *Reuters*, 25 April 2012, available at: http://www.reuters.com/article/2012/04/25/germany-cyber-idUSL6E8FP40M20120425; Keir Giles, 'Russia's public stance on cyberspace issues', paper given at the 2012 4th International Conference on Cyber Conflict, C. Czosseck, R. Ottis and K. Ziolkowski (eds), NATO CCD COE Publications, Tallinn, 2012, available at: http://www.conflictstudies.org.uk/files/Giles-Russia_Public_Stance.pdf.

8 Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc. A/66/359 of 14 September 2011.

9 Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security.

10 Available at: http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf. Annex 1 defines 'information war' as a 'confrontation between two or more states in the information space aimed at damaging

This debate – in which all sides accuse the other of espionage and arms proliferation in an open or more or less veiled manner[11] – remains very general from the legal perspective. In particular, there is no differentiation between situations of armed conflict and other situations, although the applicability of IHL depends on such a differentiation. Much of the concern appears to concentrate on espionage, against the state as well as against economic interests, but there is also talk of cyber warfare and a need to avoid weapons proliferation in cyber space. There is generally no differentiation between situations of armed conflict and other situations in which cyber operations threaten the security of states, businesses, or private households. Most debates on cyber security do not even mention situations of armed conflict, and it is unclear whether such situations are implicitly included. Indeed, in many respects, especially in relation to the protection of computer infrastructure against infiltration, manipulation, or damage, it makes no difference whether a cyber attack is carried out in the context of an armed conflict or not. The technical means of protecting the infrastructure will mostly be the same. However, while it is probably fair to say that most of the threats in the cyber realm are not immediately related to situations of armed conflict but stem, rather, from economic or other espionage, or organized cyber crime, it is also clear that recourse to cyber weapons and cyber operations is playing a growing role in armed conflicts and that states are actively preparing for this new development.

In the meantime, there is confusion about the applicability of IHL to cyber warfare – which might in fact stem from different understandings of the concept of cyber warfare itself, which range from cyber operations carried out in the context of armed conflicts as understood in IHL to criminal cyber activities of all kinds. Some states, like the US,[12] the United Kingdom of Great Britain and

information systems, processes and resources, critical and other structures, undermining political, economic and social systems, mass psychologic brainwashing to destabilize society and state, as well as to force the state to taking decision in the interest of an opposing party'. Annex 2 describes the threat of 'development and use of information weapons, preparation for and waging information war' as emanating 'from creating and developing information weapons that pose an immediate danger to critical structures of States which might lead to a new arms race and represents a major threat in the field of international information security. Among its characteristics are the use of information weapons to prepare and wage information war, and impact transportation, communication and air control systems, missile defence and other types of defence facilities, as a result of which the state looses its defence capabilities in the face of the aggressor and fails to exercise its legitimate right to self-defence; breaching information infrastructure operation, which leads to the collapse of administrative and decision-making systems in the states; and destructive impact on critical structures'.

11 Kenneth Lieberthal and Peter W. Singer, 'Cybersecurity and US–China relations', in *China US Focus*, 23 February 2012, available at: http://www.chinausfocus.com/library/think-tank-resources/us-lib/peacesecurity-us-lib/brookings-cybersecurity-and-u-s-china-relations-february-23-2012/; Mandiant Intelligence Centre Report, *APT1: Exposing one of China's Cyber Espionage Units*, available at: http://intelreport.mandiant.com/?gclid=CKD6-7Oo3LUCFalxOgod8y8AJg; Ellen Nakashima, 'US said to be target of massive cyber-espionnage campaign', in *The Washington Post*, 11 February 2013; 'North Korea says US "behind hack attack"', in *BBC News*, 15 March 2013.

12 Harold Koh, 'International law in cyberspace', speech at the US Cyber Command Inter-Agency Legal Conference, 18 September 2012, available at: http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/; Report of the Secretary-General on Developments in the field of information and telecommunication in the context of international security (hereinafter 'Report of the Secretary-General'), 15 July 2011, UN Doc. A/66/152, p. 19; see also, US Department of Defense Strategy for Operating in Cyberspace: 'Long-standing international norms guiding state behaviour – in times of

Northern Ireland,[13] and Australia,[14] have stated that IHL applies to cyber warfare.[15] However, the public positions do not yet go into detail about questions such as the threshold for armed conflicts, the definition of 'attacks' in IHL, or the implications of cyber warfare with respect to so-called dual-use objects. It has been said that China does not accept the applicability of IHL to cyber warfare.[16] However, it is unclear whether this would really be China's official position in a situation of armed conflict within the meaning of IHL. Another view is that:

> China's stance is that the nations of the world should cherish the value of cyber space – the first social space created by humankind – and should firmly oppose the militarization of the Internet. . . . Its view is that the current UN Charter and the existing laws of armed conflict as well as the basic principles of International Humanitarian Law that relate to war and the use or threat of force all still apply to cyberspace – in particular the 'no use of force' and 'peaceful settlement of international disputes' imperatives as well as the principles of distinction and proportionality in regards to the means and methods of warfare.[17]

As far as can be seen, the Russian Federation has not taken an official stance on the applicability of IHL to cyber warfare.[18]

From a legal point of view, it is important to distinguish between cyber warfare in the sense of cyber operations conducted in the context of armed conflicts

peace and conflict – also apply in cyberspace. Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them', US Department of Defense Strategy for Operating in Cyberspace, July 2011, available at: http://www.defense.gov/news/d20110714cyber.pdf.

13 Report of the Secretary-General, 23 June 2004, UN Doc. A/59/116, p. 11; Report of the Secretary-General, 20 July 2010, UN Doc. A/65/154, p. 15.

14 Report of the Secretary-General, above note 12, p. 6.

15 See also, the proposal by the High Representative of the European Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace*, Brussels, 7.2.2013, JOIN (2013) 1 final.

16 See, e.g., Adam Segal, 'China, international law and cyber space', in *Council on Foreign Relations*, 2 October 2012, available at: http://blogs.cfr.org/asia/2012/10/02/china-international-law-and-cyberspace/.

17 Li Zhang, 'A Chinese perspective on cyber war', in this edition. In his speech to the First Committee in September 2011, China's Ambassador stated that China proposed that countries 'commit themselves to non-use of information and cyber technology to engage in hostile activities to the detriment of international peace and security, and to non-proliferation of information and cyber weapons' and 'work to keep information and cyber space from becoming a new battlefield'; there is no mention of IHL. See the statement on information and cyberspace security made by H. E. Ambassador Wang Qun to the First Committee during the 66th Session of the General Assembly, 'Work to build a peaceful, secure and equitable information and cyber space', New York, 20 October 2011, available at: http://www.fmprc.gov.cn/eng/wjdt/zyjh/t869580.htm.

18 The reported military doctrine of the Russian Federation does not mention IHL with respect to information warfare; see 'The Military Doctrine of the Russian Federation Approved by Russian Federation Presidential Edict on 5 February 2010', available at: http://www.sras.org/military_doctrine_russian_federation_2010; and neither does K. Giles, above note 7; Roland Heikerö, 'Emerging threats and Russian Views on information warfare and information operations', FOI Swedish Defence Research Agency, March 2010, p. 49, available at: http://www.highseclabs.com/Corporate/foir2970.pdf, reports that the Russian Federation has proposed the 'application of humanitarian laws banning attacks on non-combatants and a ban on deception in cyberspace'.

within the meaning of IHL and cyber operations outside such contexts. It is only in the context of armed conflicts that the rules of IHL apply, imposing specific restrictions on the parties to the conflict.[19] Thus, in this article the term 'cyber warfare' will refer to means and methods of warfare that consist of cyber operations amounting to or conducted in the context of an armed conflict within the meaning of IHL only. Such cyber operations – also frequently referred to as computer network attacks – are directed against or sent via a computer or a computer system through a data stream.[20] They can aim to do different things, for instance to infiltrate a computer system and collect, export, destroy, change, or encrypt data, or to trigger, alter, or otherwise manipulate processes controlled by the infiltrated system. In other words, the following analysis deals with hostilities that consist of developing and sending computer code from one or more computers to the target computers.

The humanitarian concern

The International Committee of the Red Cross' (ICRC) humanitarian concern in respect of cyber warfare relates mainly to the potential impact on the civilian population, in particular because cyber operations could seriously affect civilian infrastructure[21] as a result of several features peculiar to the cyber realm.

First, because of its increasingly ubiquitous reliance on computer systems, civilian infrastructure is highly vulnerable to computer network attacks. In particular, a number of critical installations, such as power plants, nuclear plants, dams, water treatment and distribution systems, oil refineries, gas and oil pipelines, banking systems, hospital systems, railroads, and air traffic control rely on so-called supervisory control and data acquisition (or SCADA) systems and distributed control systems (DCS). These systems, which constitute the link between the digital and the physical worlds, are extremely vulnerable to outside interference by almost any attacker.[22]

19 For the International Committee of the Red Cross (ICRC), it is important to draw attention to the specific situation of cyber operations amounting to or conducted in the context of armed conflicts – that is, cyber warfare in a narrow sense. This is because the ICRC has a specific mandate under the 1949 Geneva Conventions to assist and protect the victims of armed conflicts. It is also mandated by the international community to work for the understanding and dissemination of IHL. See, e.g., GC III, Art. 126(5), GC IV, Art. 143(5), and Statutes of the International Red Cross and Red Crescent Movement, Art. 5(2)(g).

20 US Department of Defense, *Dictionary of Military and Associated Terms*, 8 November 2010 (as amended on 31 January 2011), Washington, DC, 2010: 'Computer network attacks are actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.'

21 In the law on the conduct of hostilities, 'civilians', 'civilian population', and 'civilian objects' are different legal concepts to which different rules apply. However, when this article speaks about the impact of cyber warfare on the civilian population, it also refers to damage done to civilian infrastructure, which is the most likely way that cyber operations will affect the civilian population.

22 Stefano Mele analyses likely scenarios of interference with different types of military and civilian systems and states that the manipulation of electrical grid management systems is probably the greatest threat at present. See Stefano Mele, 'Cyber warfare and its damaging effects on citizens', September 2010, available at: http://www.stefanomele.it/public/documenti/185DOC-937.pdf.

Second, the interconnectivity of the Internet poses a threat to civilian infrastructure. Indeed, most military networks rely on civilian, mainly commercial, computer infrastructure, such as undersea fibre optic cables, satellites, routers, or nodes; conversely, civilian vehicles, shipping, and air traffic controls are increasingly equipped with navigation systems relying on global positioning system (GPS) satellites, which are also used by the military. Thus, it is to a large extent impossible to differentiate between purely civilian and purely military computer infrastructure. As will be seen below, this poses a serious challenge to one of the cardinal principles of IHL, namely the principle of distinction between military and civilian objects. Moreover, even if military and civilian computers or computer systems are not entirely one and the same, interconnectivity means that the effects of an attack on a military target may not be confined to this target. Indeed, a cyber attack may have repercussions on various other systems, including civilian systems and networks, for instance by spreading malware (malicious software) such as viruses or worms if these are uncontrollable. This means that an attack on a military computer system may well also damage civilian computer systems, which, in turn, may be vital for some civilian services such as water or electricity supply or the transfer of assets.

For the time being, we have no clear examples of cyber attacks during armed conflicts or examples in which the civilian population has been severely affected by computer network attacks during armed conflicts. However, technical experts seem to agree that it is technically feasible, even if difficult, to deliberately interfere with airport control systems, other transportation systems, dams, or power plants via cyber space. Potentially catastrophic scenarios, such as collisions between aircraft, the release of radiation from nuclear plants, the release of toxic chemicals from chemical plants, or the disruption of vital infrastructure and services such as electricity or water networks, cannot be discarded.

Such scenarios might not be the most likely ones; cyber operations are in all probability more likely to be used to manipulate civilian infrastructure leading it to malfunction or disrupting it without causing immediate death or injury. The effects of such 'bloodless' means and methods of warfare might not be as dramatic for civilians as shelling or bombing. They can nevertheless be severe – for instance, if the power or water supply is interrupted, or if communication networks or the banking system are down. These effects and how they must be taken into account under the rules of IHL must therefore be clarified.

Some commentators have argued that the threat of computer network attacks on the larger civilian infrastructure should not be overstated, in particular, because offensive cyber weapons would often need to be very specifically written to affect specific target computer systems (like the Stuxnet virus, for instance)[23] and

23 The so-called Stuxnet virus was launched against the Iranian uranium enrichment facility at Natanz, reportedly leading to the destruction of a thousand centrifuges. It is reported in the press that the United States and/or Israel were behind this virus, but this has not been officially acknowledged. David Albright, Paul Brannan and Christina Walrond, 'Did Stuxnet take out 1,000 centrifuges at the Natanz enrichment plant? Preliminary assessment', ISIS Report, 22 December 2010, available at: http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/; David E. Sanger, 'Obama order sped up wave of cyberattacks against Iran', in *The New York Times*, 1 June 2012,

could therefore not easily be redirected at other targets.[24] Also, in an internationally interconnected Internet system and in a globalized economy, states might be reluctant to damage each other because the repercussions, for instance on financial systems, might damage them as much as their adversary.[25] That might or might not be the case. The fact that computer network attacks are potentially capable of targeting civilian objects, might in some instances be indiscriminate or be used in an indiscriminate manner, or could potentially have devastating incidental consequences for civilian infrastructure and the civilian population is reason enough to clarify the applicable rules on the conduct of hostilities that parties to conflicts must observe.

The role of international humanitarian law

Against this background, how does IHL address the potential consequences of cyber warfare on the civilian population?

IHL provisions do not specifically mention cyber operations. Because of this, and because the exploitation of cyber technology is relatively new and sometimes appears to introduce a complete qualitative change in the means and methods of warfare, it has occasionally been argued that IHL is ill adapted to the cyber realm and cannot be applied to cyber warfare.[26] However, the absence in IHL of specific references to cyber operations does not mean that such operations are not subject to the rules of IHL. New technologies of all kinds are being developed all the time and IHL is sufficiently broad to accommodate these developments. IHL prohibits or limits the use of certain weapons specifically (for instance, chemical or biological weapons, or anti-personnel mines). But it also regulates, through its general rules, all means and methods of warfare, including the use of all weapons. In particular, Article 36 of Protocol I additional to the Geneva Conventions provides that:

> [i]n the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.

available at: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran. html?pagewanted=all&_moc.semityn.www.

24 Thomas Rid, 'Think again: cyberwar', in *Foreign Policy*, March/April 2012, pp. 5 *ff*., available at: http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?print=yes&hidecomments=yes&page=full; Thomas Rid and Peter McBurney, 'Cyber-weapons', in *The RUSI Journal,* February–March 2012, Vol. 157, No. 1, pp. 6–13; see also, Maggie Shiels, 'Cyber war threat exaggerated claims security expert', in *BBC News*, 16 February 2011, available at: http://www.bbc.co.uk/news/technology-12473809.

25 Stefano Mele (above note 22) argues that for this reason massive electronic attacks against financial systems of foreign countries are unlikely.

26 Charles J. Dunlap Jr., 'Perspectives for cyber strategists on law for cyberwar', in *Strategic Studies Quarterly*, Spring 2011, p. 81.

Beyond the specific obligation it imposes on states party to Additional Protocol I, this rule shows that IHL rules apply to new technology.

That said, cyber warfare challenges some of the most fundamental assumptions of IHL. First, IHL assumes that the parties to conflicts are known and identifiable. This cannot always be taken for granted even in traditional armed conflicts, in particular, non-international armed conflicts. However, in the cyber operations that occur on an everyday basis, anonymity is the rule rather than the exception. It appears to be impossible in some instances to trace their originator, and even when this is possible it is in most cases time-consuming. Since all law is based on the allocation of responsibility (in IHL, to a party to a conflict or to an individual), major difficulties arise. In particular, if the perpetrator of a given operation and thus the link of the operation to an armed conflict cannot be identified it is extremely difficult to determine whether IHL is even applicable to the operation. So, for instance, if a government's infrastructure is being attacked, but it is not clear who is behind the attack, it is difficult to define who the parties to the potential armed conflict are, and therefore to determine whether there is an armed conflict at all. Similarly, even if the parties to the conflict are known, it may be difficult to attribute the act to one particular party. Second, IHL is based on the assumption that the means and methods of warfare will have violent effects in the physical world. Many cyber operations are likely to have effects that are disruptive but not immediately perceivably physically destructive. Third, the entire structure of the rules on the conduct of hostilities – and in particular the principle of distinction – is founded on the assumption that civilian objects and military objects are, for the most part, distinguishable. In the cyber theatre of war this is likely to be the exception rather than the rule because most cyber infrastructure around the world (undersea cables, routers, servers, satellites) serves for both civilian and military communications.

The following analysis therefore seeks to explore how the rules of IHL can be interpreted to make sense in the cyber realm, and how cyber technology might touch upon their limits. As will be shown below, it is probably too early to give definite answers to many of the questions raised because examples are few and the facts not entirely clear and state practice with respect to the interpretation and implementation of applicable norms still has to evolve. To date, the Tallinn Manual on the International Law Applicable to Cyber Warfare (hereinafter 'Tallinn Manual') is the most comprehensive exercise seeking to interpret the rules of international law (*jus ad bellum* and *jus in bello*) to cyber warfare.[27] It was drafted by a group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, and provides a useful compilation of rules with commentary reflecting the different views on some of the thorny issues raised by this new technology. The ICRC took part in the deliberations of the group of experts as an observer, but does not endorse all the views expressed in the Manual.

27 Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013 (forthcoming). The *Tallinn Manual* is available at: http://www.ccdcoe.org/249.html.

Applicability of international humanitarian law to cyber operations: what is an armed conflict in cyber space?

IHL is only applicable if cyber operations are conducted in the context of and related to an armed conflict. Thus, it should be fairly uncontroversial that when cyber operations are conducted in the context of an ongoing armed conflict they are governed by the same IHL rules as that conflict: for instance, if in parallel or in addition to a bomb or missile attack, a party to the conflict also launches a cyber attack on the computer systems of its adversary.

However, a number of operations referred to as cyber warfare may not be carried out in the context of armed conflicts at all. Terms like 'cyber attacks' or 'cyber terrorism' may evoke methods of warfare, but the operations they refer to are not necessarily conducted in an armed conflict. Cyber operations can be and are in fact used in crimes committed in everyday situations that have nothing to do with war.

Other situations that fall between situations of existing armed conflicts fought with traditional means and cyber operations and situations that are entirely outside the realm of armed conflict are harder to classify. This is the case, in particular, when computer network attacks are the only hostile operations carried out and even more so if they remain isolated acts. This scenario is not entirely futuristic. The Stuxnet virus, which appears to have targeted the uranium enrichment facility of the Islamic Republic of Iran at Natanz, has remained, for the time being, an isolated computer network attack (even if carried out over a period of time), possibly launched by one or more states against the Islamic Republic of Iran. While classification as an armed conflict has not arisen in the discourse of states, the reasoning of some commentators suggested that if carried out by a state, this attack would amount to an international armed conflict.[28] Another conceivable scenario would be large-scale and sustained cyber operations conducted by a non-state organised armed group against government infrastructure. Can such operations rise to the level of a non-international armed conflict?

Under existing IHL, there are two – and only two – types of armed conflict: international armed conflicts and non-international armed conflicts. Not all criteria for the existence of such conflicts will be discussed here. Instead, some aspects that seem to raise particularly difficult questions with respect to cyber operations will be addressed.

International armed conflicts

Under common Article 2 to the four Geneva Conventions of 1949, an international armed conflict is any 'declared war or any other armed conflict which may arise

28 Michael N. Schmitt, 'Classification of cyber conflict', in *Journal of Conflict and Security Law*, Vol. 17, Issue 2, Summer 2012, p. 252; see also, Gary Brown, 'Why Iran didn't admit Stuxnet was an attack', in *Joint Force Quarterly*, Issue 63, 4th Quarter 2011, p. 71, available at: http://www.ndu.edu/press/why-iran-didnt-admit-stuxnet.html. G. Brown does not address the question of conflict classification, but considers that Stuxnet clearly amounted to an attack, possibly in violation of the prohibition against the use of force and the law of war.

INTERNATIONAL REVIEW of the Red Cross

between two or more States even if the state of war is not recognized by one of them'. There is no further treaty definition of international armed conflicts and it is by now accepted that, in the words of the International Criminal Tribunal for the former Yugoslavia (ICTY), an international armed conflict arises 'whenever there is a *resort to armed force* between States'.[29] The application of IHL depends on the factual situation and not on the recognition of a state of armed conflict by the parties thereto.

The specific question that arises in cyber warfare is whether an international armed conflict can be triggered by a computer network attack in the absence of any other (kinetic) use of force. The answer depends on whether a computer network attack is (1) attributable to the state and (2) amounts to a resort to armed force – a term that is not defined under IHL.

Attribution of conduct to the state

The question of attribution of an operation to a state could raise particularly difficult questions in cyber space where anonymity is the rule rather than the exception. Yet, as long as the parties cannot be identified as two or more states it is impossible to classify the situation as an international armed conflict. While this is a challenge in factual rather than in legal terms, a way of overcoming the uncertainty in fact would be through legal presumptions. For instance, if a computer network attack originated from the government infrastructure of a particular state, a presumption could be drawn that the operation is attributable to the state – especially in light of the rule of international law that states must not knowingly allow their territory to be used for acts contrary to the rights of other states.[30] There are, however, two objections to this approach.

First, the existing rules of international law do not support such a presumption. For instance, the Articles on Responsibility of States for Internationally Wrongful Acts of the International Law Commission do not contain rules on presumption of attribution of conduct to a state. Also, the International Court of Justice (ICJ) set a high threshold for attribution of conduct to a state in the context of the right to self-defence. In the *Oil Platforms* case, it effectively held that the burden of proof rests on the state invoking the right of self-defence:

> Court has simply to determine whether the United States has demonstrated that it was the victim of an 'armed attack' by Iran such as to justify it using armed force in self-defence; and the burden of proof of the facts showing the existence of such an attack rests on the United States.[31]

29 International Criminal Tribunal for the Former Yugoslavia (ICTY), *Prosecutor* v. *Tadic*, Case No. IT-94-1-A, Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995, para. 70 (emphasis added). The situations foreseen in Article 1(4) AP I are also considered international armed conflicts for States Party to AP I.

30 International Court of Justice (ICJ), *Corfu Channel* case (*United Kingdom* v. *Albania*), Judgment of 9 April 1949, p. 22; see also, Rule 5 of the *Tallinn Manual*, above note 27.

31 ICJ, *Oil Platforms* case *(Islamic Republic of Iran* v. *United States of America)*, Judgment of 6 November 2003, para. 57.

While this statement was made in the context of the right to self-defence in *jus ad bellum*, it can be generalized to all factual questions of attribution of conduct to a state. Since it is a presumption about facts, it would be nonsensical to presume facts for one purpose and not for another.

Second, such a presumption would also be too far-reaching in the particular context of cyber warfare. Given the difficulty of shielding computer infrastructure from manipulation and the ease with which one can remotely control a computer and pose under a different identity in cyber space, it would be placing a very high burden on governments to hold them accountable for all operations originating from their computers without any further proof.[32]

Another more frequently discussed question is the attribution of cyber attacks launched by private parties, such as hacker groups, to the state. Apart from the factual questions raised by the anonymity of cyber operations, the legal rules for attribution of acts of private parties to a state are set out in the Articles on Responsibility of States for Internationally Wrongful Acts.[33] In particular, a state is responsible for the conduct of a person or group of persons 'if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct'.[34] What exactly 'direction or control' means in international law will have to be clarified over time. The ICJ requires that for an act of a private party (be it an individual or a member of an organised group) to be imputable to the state the direction or effective control of the state over the operation in the course of which the alleged violations were committed has to be demonstrated, and not only generally in respect of the overall actions taken by the persons or groups of persons having committed the violations.[35] In the absence of such control over the specific operation it cannot be imputed to the state, even when committed by a group with a high degree of dependency on the state authorities.[36] In the same vein, the commentary on the Articles on State Responsibility requires that the state direct or control the specific operation and that the conduct be an integral part of that operation.[37] The ICTY has gone further and argued that where a group, such as an armed opposition group, is organised it is enough that the state authorities exercise 'overall control' over such an organised and hierarchically

32 The *Tallinn Manual* takes a similar legal view in Rule 7: 'The mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State but is an indication that the State in question is associated with the operation'.

33 International Law Commission, Draft Articles on the Responsibility of States for Internationally Wrongful Acts, *Yearbook of the International Law Commission*, 2001, Vol. II (Part Two). Text reproduced as it appears in the annex to General Assembly resolution 56/83 of 12 December 2001, and corrected by document A/56/49(Vol. I)/Corr.4 (hereinafter 'Articles on State Responsibility').

34 Article 8 of the Articles on State Responsibility.

35 ICJ, *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua* v. *United States of America*), Judgment of 27 June 1986, paras 115–116 (hereinafter '*Nicaragua* case'); ICJ, *Case concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (*Bosnia and Herzegovina* v. *Serbia and Montenegro*), Judgment, 26 February 2007, paras 400–406.

36 *Nicaragua* case, above note 35, para. 115.

37 Report of the International Law Commission on the work of its fifty-third session (23 April–1 June and 2 July–10 August 2001), UN Doc. A/56/10, Commentary on Article 8 of the Draft Articles on State Responsibility, para 3.

structured group without a need for specific control or direction over individual conduct.[38] However, the ICTY has also acknowledged that where the controlling state is not the territorial state, 'more extensive and compelling evidence is required to show that the State is genuinely in control of the units and groups' – meaning that the state's involvement in the planning of military operations or its coordination role might be more difficult to demonstrate.[39] The International Law Commission's commentary states: 'it will be a matter of appreciation in each case whether particular conduct was or was not carried out under the control of a State, to such an extent that the conduct controlled should be attributed to it'.[40] This discussion, however, is not specific to the cyber domain. Once the facts are established, the same legal criteria apply as with any other attribution of the conduct of private parties to a state. The difficulty, here again, will most likely lie in the factual assessment.

Resort to armed force

The second criterion to be fulfilled is that of 'resort to armed force' between states.

Before turning to the questions raised by cyber warfare in this respect, it is worth clarifying very briefly that the classification of a conflict as an international armed conflict under IHL (*jus in bello*) is separate from the question of *jus ad bellum*. The two are often amalgamated, including in cyber warfare.

Under *jus ad bellum*, the question is whether and when cyber operations amount to a use of force within the meaning of Article 2(4) of the UN Charter and/or to an armed attack within the meaning of Article 51 of the UN Charter, and under what circumstances they trigger a right to self-defence.[41] Whatever the views in this *jus ad bellum* discussion, it should be recalled that the objects of regulation of *jus ad bellum* and *jus in bello* are entirely distinct: while *jus ad bellum* specifically regulates inter-state relations and the requirements for the lawful resort to force between states, *jus in bello* regulates the behaviour of parties to the conflict and its object and purpose is to protect the military and civilian victims of war. Thus, an act could constitute a resort to armed force for the purpose of qualifying an international armed conflict, without prejudice to the question whether it also constitutes a use of force within the meaning of Article 2(4) of the UN Charter

38 ICTY, *Prosecutor* v. *Dusko Tadic*, IT-94-1, Appeals Chamber Judgment of 15 July 1999, para. 120. It is sometimes said that the question before the Tribunal was one of qualification of the conflict as non-international or international; however, the argument that the two questions are entirely separate is not convincing as it would lead to the conclusion that a state could be a party to a conflict by virtue of its control over an organized armed group but not be responsible for the acts committed during that conflict.

39 *Ibid.*, paras 138–140.

40 Commentary on Article 8 of the Draft Articles on State Responsibility, above note 37, para. 5.

41 See Marco Roscini, 'World wide warfare – *jus ad bellum* and the use of cyber force', in *Max Planck Yearbook of United Nations Law*, Vol. 14, 2010, p. 85; Michael N. Schmitt, 'Computer network attack and the use of force in international law: thoughts on a normative framework', in *Columbia Journal of Transnational Law*, Vol. 37, 1998–1999, p. 885; Herbert S. Lin, 'Offensive cyber operations and the use of force', in *Journal of National Security Law and Policy*, Vol. 4, 2010, p. 63; David P. Fidler, 'Recent developments and revelations concerning cybersecurity and cyberspace: implications for international law', in *ASIL Insights*, 20 June 2012, Vol. 16, no. 22; *Tallinn Manual*, above note 27, Rules 10–17.

(though it is likely), let alone an armed attack under Article 51. This differentiation equally applies to cyber operations.

Turning to *jus in bello*, there is no treaty definition of the meaning of armed force in IHL because it is a jurisprudential criterion. Traditionally, the objective of war is to prevail over the enemy, and in traditional warfare, conflict entails the deployment of military means, leading to military confrontation. Thus, when traditional means or methods of warfare are used – such as bombing, shelling, or the deployment of troops – it is uncontroversial that these amount to armed force. But computer network attacks do not entail the use of such arms.

In the absence of traditional weapons and kinetic force – what can be considered to amount to armed force in the cyber realm?

The first step is to compare the analogous effects of computer network attacks to those of kinetic force. Most commentators are of the view that if a computer network attack is attributable to a state and has the same effects as kinetic resort to force it would trigger an international armed conflict.[42] Indeed, if a computer network attack causes airplanes or trains to collide, resulting in death or injury, or widespread flooding with large-scale consequences, there would be little reason to treat the situation differently from equivalent attacks conducted through kinetic means or methods of warfare.

This parallel is therefore useful for situations in which computer network attacks lead to death or injury, or physical damage or destruction of infrastructure. However, it might be insufficient to capture the whole range of possible effects of cyber operations and the damage that they can cause, which will not necessarily resemble the physical effects of traditional weapons. Cyber operations will frequently be resorted to in order not to physically destroy or damage military or civilian infrastructure, but rather to affect its functioning, for instance by manipulating it, and even to do so without the manipulation being detected. For instance, an electrical grid might be left untouched physically but nonetheless be put out of commission by a computer network attack. Similarly, a country's banking system might be manipulated without any of the infrastructure being damaged physically and without the manipulation of the underlying system even being noticeable for some time. At first sight, even in the absence of traditional military means or of immediate physical destruction, the potential effects of such disruptions – which might be far more extensive or severe than, say, the destruction of a particular building or group of buildings – on the population would speak in favour of considering them a resort to armed force. However, states – even victim states – might seek to avoid an escalation of international confrontations or have

42 M. N. Schmitt, 'Classification of cyber conflict', above note 28, p. 251; Knut Dörmann, 'Applicability of the Additional Protocols to Computer Network Attacks', ICRC, 2004, p. 3, available at: http://www.icrc.org/eng/resources/documents/misc/68lg92.htm; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge, 2012, p. 131; Nils Melzer, *Cyberwarfare and International Law*, UNIDIR Resources Paper, 2011, p. 24, available at: http://www.unidir.ch/pdf/ouvrages/pdf-1-92-9045-011-L-en.pdf. Nils Melzer argues that since the existence of an international armed conflict depends mainly on the occurrence of armed hostilities between states, cyber operations would trigger an armed conflict not only by death, injury, or destruction, but also by directly adversely affecting the military operations or military capacity of the state.

other reasons to avoid treating such types of attacks as triggering an armed conflict. It is difficult at this point to infer any legal positions, since states appear to remain mostly silent in the face of cyber attacks.[43] In the absence of clear state practice there are several possible approaches to this question.

One approach is to consider any hostile cyber operation that affects the functioning of objects as a resort to armed force. The object and purpose of IHL in general, and in particular the absence of a threshold of violence for the existence of an international armed conflict – which is to avoid a gap in protection, particularly the protection of the civilian population from the effects of war – would speak in favour of including such cyber operations in the definition of armed force for the purpose of triggering an armed conflict. Also, considering the importance that states attach to the protection of critical infrastructure in their cyber strategies, it might well be the case that they will consider computer network attacks by another state aimed at incapacitating such infrastructure as the beginning of an armed conflict.[44] Moreover, in the absence of an armed conflict the protective scope of IHL would not govern the situation. Other bodies of law such as *jus ad bellum*, cyber crime law, space law, or telecommunications law might, of course, apply and provide their own protection. The analysis of their effect is beyond the scope of this article, but all of the other bodies of law would pose their own set of questions. For instance, international human rights law might apply, but would a computer network attack, conducted from the other side of the globe against civilian infrastructure, fulfil the requirement of effective control for the purpose of applicability of human rights law? Also, to what extent would human rights law provide sufficient protection against the disruption of infrastructure the effects of which on the lives of civilians is not necessarily immediately identifiable?

Another approach would be to not focus exclusively on the analogous effects of the cyber operation but to consider a combination of factors that would indicate armed force. These factors would include a certain severity of the consequences of the cyber operation, the means employed, the involvement of the military or other parts of the government in the hostile operation, the nature of the target (military or not), and the duration of the operation. Taking an example outside of the cyber realm, if the chief of staff of a state's armed forces was killed in an air attack by another state this would certainly be considered as amounting to an international armed conflict. However, if he or she was killed by the sending of a

43 See also, G. Brown, above note 28.

44 N. Melzer, above note 42, p. 14. Melzer argues that reference might be made to the concept of critical infrastructure to consider the 'scale and effects' of a computer network attack for the purposes of identifying an armed attack within the meaning of Article 51 of the UN Charter. For French policy, see Agence Nationale de la Sécurité des Systèmes d'Information, *Défense et sécurité des systèmes d'informations,* available at: http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf; for German policy, see Bundesamt für Sicherheit in der Informationstechnik, *Schutz Kritischer Infrastrukturen*, available at: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Strategie/Kritis/Kritis_node.html; for Canadian policy, see *National Strategy for Critical Infrastructure*, available at: http://www.publicsafety.gc.ca/prg/ns/ci/ntnl-eng.aspx; for the policy of the United Kingdom, see *The UK Cyber Security Strategy*, available at: http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy; for Australian policy, see CERT Australia, *Australia's National Computer Emergency Response Team*, available at: https://www.cert.gov.au/.

poisoned letter would this also be considered in and of itself as amounting to an international armed conflict?[45] What if the target was a civilian? Are the means of destroying infrastructure relevant? For instance, if parts of a nuclear installation were sabotaged by infiltrated foreign agents, would this also amount to a resort to armed force? Does it make a difference whether the target is military or civilian?

In the cyber realm, it is possible, for instance, that states might treat computer network attacks on their military infrastructure differently from those affecting civilian systems. This might not be entirely technically logical because use of force is use of force, whether against a civilian or a military object. But the threshold of harm that states are willing to tolerate might be lower when it comes to operations that are targeted at and degrade their military capability.

Following such an approach, if the computer network attack is only punctual and of short duration, it may be that it will only be considered as armed force if its consequences are of a particular severity. The example of the Stuxnet attack as reported in the press seems to indicate that computer network attacks might – at least for some time – remain isolated hostile acts of one state towards another, without other kinetic operations, particularly if the attacker wishes to remain anonymous, wishes for the attack to remain undetected for some time, or wishes (for political or other reasons) to avoid an escalation of force and further hostilities and armed conflict. If one relied solely on whether a kinetic attack with the same effects amounts to armed force, one might have to come to the conclusion that such an attack constitutes armed force because the Stuxnet virus is reported to have caused the physical destruction of about one thousand IR-1 centrifuges which had to be replaced at the uranium enrichment facility at Natanz.[46] Indeed, if the centrifuges of a nuclear installation were destroyed by bombardment by another state's air force, such an attack would be considered a resort to armed force and trigger an international armed conflict. But because the means of the attack were not kinetic, no other attacks in connection to it were reported and it caused no known damage beyond the centrifuges, it arguably falls short of armed force triggering an international armed conflict.

To sum up, it remains to be seen if and under what conditions states will treat computer network attacks as armed force. The mere manipulation of a banking system or other manipulation of critical infrastructure, even if it leads to serious economic loss, would probably stretch the concept of armed force beyond its object and purpose – the effects are not equivalent to the destruction caused by physical means. But the disruption of such vital infrastructure as electricity or water supply systems, which would inevitably lead to severe hardship for the population if it lasted over a certain period, even if not to death or injury, might well have to be

45 In *How Does Law Protect in War?*, Vol. I, 3rd edn, ICRC, Geneva, 2011, p. 122, Marco Sassòli, Antoine Bouvier, and Anne Quintin differentiate between force by the military or other agents of the state: '[w]hen the armed forces of two States are involved, suffice for one shot to be fired or one person captured (in conformity with government instructions) for IHL to apply, while in other cases (e.g. a summary execution by a secret agent sent by his government abroad), a higher level of violence is necessary'.

46 This is the opinion of M. N. Schmitt, above note 28, p. 252; on the damage caused see D. Albright, P. Brannan and C. Walrond, above note 23; D. E. Sanger, above note 23.

considered as armed force. Although the effects are not equivalent to physical effects, they are precisely the kind of severe consequences from which IHL seeks to protect the civilian population.

It is true that states cannot circumvent their obligations under IHL by their own designation of the act. The application of the law of international armed conflict was divorced from the need for official pronouncements many decades ago in order to avoid cases in which states could deny the protection of this body of rules. This is made clear by common Article 2, as the ICRC Commentary thereto suggests:

> [a] State can always pretend, when it commits a hostile act against another State, that it is not making war, but merely engaging in a police action, or acting in legitimate self-defence. The expression 'armed conflict' makes such arguments less easy.[47]

Nonetheless, while it is true that in a specific incident, the classification of the conflict does not depend on the position of the states concerned, state practice and *opinio juris* determine the interpretation of the international law definition of 'international armed conflicts'.The classification of cyber conflicts will probably be determined in a definite manner only through future state practice.

Non-international armed conflicts

When it comes to non-international armed conflicts in the cyber realm, the main question is how to differentiate between criminal behaviour and armed conflict. It is not rare to hear or read about the actions of hacker or other groups, including groups such as Anonymous or Wikileaks, being referred to as 'war'.[48] Of course, such statements do not necessarily allude to armed conflict, or more precisely non-international armed conflict, in a legal sense. Nevertheless, it is worth clarifying the parameters for qualifying a situation as a non-international armed conflict.

In the absence of a treaty definition, state practice and doctrine has led to a definition of non-international armed conflicts that the ICTY has summed up as follows: a non-international armed conflict exists 'whenever there is … protracted armed violence between governmental authorities and organised armed groups or between such groups within a State'.[49] The 'protracted' requirement has with time

47 Jean Pictet (ed.), *Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, ICRC, Geneva, 1952, p. 32. This is a different question from that of *animus belligerendi*: isolated acts are sometimes not considered to amount to armed conflict, not because they do not reach a certain level of intensity, but rather because they lack *animus belligerendi*, for instance accidental border incursions; see *UK Joint Service Manual of the Law of Armed Conflict*, Joint Service Publication 383, 2004, para. 3.3.1, available at: http://www.mod.uk/NR/rdonlyres/82702E75-9A14-4EF5-B414-49B0D7A27816/0/JSP3832004Edition.pdf.

48 See, e.g., Mark Townsend *et al.*, 'WikiLeaks backlash: The first global cyber war has begun, claim hackers', in *The Observer*, 11 September 2010, available at: http://www.guardian.co.uk/media/2010/dec/11/wikileaks-backlash-cyber-war; Timothy Karr, 'Anonymous declares cyberwar against "the system"', in *The Huffington Post*, 3 June 2011, available at: http://www.huffingtonpost.com/timothy-karr/anonymous-declares-cyberw_b_870757.html.

49 ICTY, *Prosecutor* v. *Tadic*, above note 29, para. 70.

been subsumed under a requirement that the violence must reach a certain intensity. Thus, two criteria determine the existence of a non-international armed conflict: the armed confrontation must reach a minimum level of intensity and the parties involved in the conflict must show a minimum of organisation.[50]

Organised armed groups

For a group to qualify as an organised armed group that can be a party to a conflict within the meaning of IHL, it needs to have a level of organisation that allows it to carry out sustained acts of warfare and comply with IHL. Indicative elements include the existence of an organisational chart indicating a command structure, the authority to launch operations bringing together different units, the ability to recruit and train new combatants, and the existence of internal rules.[51] While the group does not need to have the level of organisation of state armed forces, it must possess a certain level of hierarchy and discipline and the ability to implement the basic obligations of IHL.[52]

With respect to hacker or other similar groups, the question that arises is whether groups that are organised entirely online can constitute armed groups within the meaning of IHL. As Michael Schmitt puts it:

> The members of virtual organisations may never meet nor even know each other's actual identity. Nevertheless, such groups can act in a coordinated manner against the government (or an organized armed group), take orders from a virtual leadership, and be highly organized. For example, one element of the group might be tasked to identify vulnerabilities in target systems, a second might develop malware to exploit those vulnerabilities, a third might conduct the operations and a fourth might maintain cyber defences against counter-attacks.[53]

However, the requirement that organised armed groups must have some form of responsible command and the capacity to implement IHL would seem to preclude virtually organised groups from qualifying as organised armed groups; it would be difficult, for instance, to establish an effective system of discipline within such a group in order to ensure respect for IHL.[54] In other words, it is unlikely that groups of hackers or groups that are merely linked by virtual communication would have

50 There are two types of non-international armed conflicts. All non-international armed conflicts are covered by common Article 3 to the Geneva Conventions; in addition, the provisions of Additional Protocol II apply to non-international armed conflicts 'which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol' (AP II, Art. 1(1)).

51 For a review of the indicative factors taken into account by the ICTY in its case law, see ICTY, *Prosecutor* v. *Boskoski*, IT-04-82-T, Trial Chamber Judgement of 10 July 2008, paras 199–203. See also, ICTY, *Prosecutor* v. *Limaj*, IT-03-66-T, Trial Chamber Judgement of 30 November 2005, paras 94–134; ICTY, *Prosecutor* v. *Haradinaj*, IT-04-84-T, Trial Chamber Judgement of 3 April 2008, para. 60.

52 ICTY, *Prosecutor* v. *Boskoski*, *ibid.*, para. 202.

53 M. N. Schmitt, above note 28, p. 256.

54 *Ibid.*, p. 257.

the organisation or command (and disciplinary) structure required to constitute a party to the conflict.[55]

Intensity

Cyber operations conducted in the context of and in relation to an existing non-international armed conflict are governed by IHL. The question that arises, although it may seem futuristic at this point, is whether the required level of intensity for a non-international armed conflict could be reached if cyber means alone are being used (assuming that there are two or more parties to the conflict).

Contrary to the classification of international armed conflicts, there is agreement that a non-international armed conflict only exists if the hostilities reach a certain level of intensity. The ICTY has pointed to a number of indicative factors to be taken into account to assess the intensity of the conflict, such as the collective character of hostilities, the resort to military force, not simply police force, the seriousness of attacks and whether there has been an increase in armed clashes, the spread of clashes over territory and over a period of time, the distribution of weapons among both parties to the conflict, the number of civilians forced to flee from the combat zones, the types of weapons used, in particular the use of heavy weapons, and other military equipment, such as tanks and other heavy vehicles, the extent of destruction and the number of casualties caused by shelling or fighting.[56] Would the necessary intensity threshold be reached by cyber operations alone?

The starting point, again, is to compare the intensity of the consequences to that of kinetic operations. There is no reason why cyber operations cannot have the same violent consequences as kinetic operations, for instance if they were used to open the floodgates of dams, or to cause aircraft or trains to collide. In such circumstances, and if such violence is not merely sporadic, it may meet the threshold for a non-international armed conflict.

However, cyber operations in themselves would not have many of the effects mentioned above as indicators of the intensity of the violence (armed clashes, the deployment of military force, heavy weapons, etc.). It would likely be the consequences of the cyber operations alone that are severe enough to reach the intensity required, such as extensive destruction or disastrous effects on large parts of the population through repeated attacks.

Summary

It is likely to be uncontroversial that IHL will apply to cyber operations that are conducted within the framework of an ongoing international or non-international armed conflict alongside kinetic operations. In the absence of kinetic operations,

55 See the discussion in the *Tallinn Manual* about the different types of groups that could be considered, above note 27, Commentary on Rule 23, paras 13–15.

56 See, *e.g.*, ICTY, *Prosecutor* v. *Limaj*, above note 51, paras 135–170; ICTY, *Prosecutor* v. *Haradinaj*, above note 51, para. 49; ICTY, *Prosecutor* v. *Boskoski*, above note 51, paras 177–178.

'pure' cyber warfare is not excluded in theory, but it remains to be seen whether there will be many examples in practice in the near future.

In particular, it remains unclear in what direction state practice will tend. Given the reluctance of states to admit situations of armed conflict, in particular non-international armed conflict, the tendency could be to avoid a discourse of armed conflict. This is not only due to the likely anonymity of many computer network attacks and the practical problems of attribution, but also to the fact that most of the situations might not amount to extreme cases of physical destruction caused by computer network attacks but rather to low-level, bloodless manipulation of infrastructure. States might choose to deal with such situations as matters of law enforcement and criminal law, and not see them as being governed by the legal framework applicable to armed conflicts.

Application of the rules on the conduct of hostilities

If cyber operations are conducted in the context of an armed conflict they are subject to the rules of IHL, in particular the rules on the conduct of hostilities. The fact that cyber weapons rely on new technologies does not by itself call into question the applicability of IHL to them.

However, cyber warfare poses serious challenges to the very premises on which IHL is predicated, in particular the distinction – and actual possibility to distinguish – between military and civilian objects. Thus, the question is not so much whether the rules on the conduct of hostilities apply to cyber warfare, but rather how they apply – how they must be interpreted to make sense in this new realm.

Which acts are subject to the IHL rules on the conduct of hostilities?

Before turning to the rules on the conduct of hostilities – in particular the principles of distinction, proportionality, and precaution – it is important to address a question that has been a subject of debate for some time, namely what type of conduct, in particular what type of cyber operation, triggers the rules on the conduct of hostilities.

The question is critical. Only if a certain cyber operation is subject to the principle of distinction is it prohibited to target it directly at civilian infrastructure; and if it is directed at a military objective, the incidental effects on the civilian infrastructure must be taken into account if the operation is subject to the principle of proportionality.

The reason why this debate arises is that cyber space is different from traditional theatres of war in that the means and methods of attack do not entail traditional kinetic force, or what is commonly understood as violence. Thus, a number of cyber operations can have a severe effect on the targeted object by disrupting its functioning, but without causing the physical damage to the object that would occur in traditional warfare.

It is therefore critical for the civilian population that this question be clarified. Depending on how narrowly or broadly one views the types of cyber

operations that are subject to the rules on the conduct of hostilities, the following could be prohibited or lawful in the context of an armed conflict:

- disrupting the civilian electrical grid or water treatment system (without physical damage thereto);
- directing a denial of service attack on an Internet banking system with significant impact on the ability of a few million bank customers to access banking services;[57]
- disrupting the website of an adversary state's stock exchange without affecting its trading functions;[58]
- directing a denial of service attack on a private airline's online booking system in order to cause inconvenience to the civilian population;
- blocking the websites of Al Jazeera or the BBC because they contain information that contributes to the enemy's operational picture;
- blocking access to Facebook for the entire population because it contains pro-insurgency propaganda;
- shutting down the Internet and cell phone networks in a specific region of a country to curb propaganda by the adversary.[59]

This leads to two questions: first, do the core rules of IHL on the conduct of hostilities – that is, the principles of distinction, proportionality, and precaution – only apply to operations that constitute attacks within the meaning of IHL, or do they apply to military operations more generally? Second, which cyber operations constitute attacks within the meaning of IHL?

What triggers the rules on the conduct of hostilities: 'attacks', 'military operations', 'hostilities'?

As to the first question, the difference in views arises from the general rule on the conduct of hostilities, as formulated in Articles 48 *et seq.* of Additional Protocol I and largely recognized as customary law. Article 48 of Additional Protocol I requires that:

> In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and

57 This occurred in Estonia in May 2007; see Larry Greenemeier, 'Estonian attacks raise concern over cyber "nuclear winter"', in *Information Week*, 24 May 2007, available at: http://www.informationweek.com/estonian-attacks-raise-concern-over-cybe/199701774.

58 See, for example, Yolande Knell, 'New cyber attack hits Israeli stock exchange and airline', in *BBC News*, 16 January 2012, available at: http://www.bbc.co.uk/news/world-16577184.

59 In Egypt, the government shut down the Internet and cell phone network for five days to curb protests: 'Internet blackouts: reaching for the kill switch', in *The Economist*, 10 February 2011, available at: http://www.economist.com/node/18112043. Similar measures were taken by the Chinese government in reaction to unrest in Xinjiang and Tibet: Tania Branigan, 'China cracks down on text messaging in Xinjiang', in *The Guardian*, 29 February 2010, available at: http://www.guardian.co.uk/world/2010/jan/29/xinjiang-china, and Tania Branigan, 'China cut off internet in area of Tibetan unrest', in *The Guardian*, 3 February 2012, available at: http://www.guardian.co.uk/world/2012/feb/03/china-internet-links-tibetan-unrest.

> military objectives and accordingly shall *direct their operations* only against military objectives. (emphasis added)

The subsequent rules on the conduct of hostilities are then mainly formulated as restrictions on attacks more specifically. For instance, Article 51 of Additional Protocol I, after stating, in its first paragraph, that '[t]he civilian population and individual civilians shall enjoy general protection against the dangers arising from military operations', goes on to state that '[t]he civilian population as such, as well as individual civilians, shall not be the object of attack' and that 'indiscriminate attacks are prohibited'. An attack in violation of the principle of proportionality is defined in Article 51(5)(b) of Additional Protocol I as 'an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated'. Article 51(6) prohibits 'attacks against the civilian population or civilians by way of reprisals'. Article 52 states that 'attacks shall be limited strictly to military objectives'. The principle of precaution in Article 57 requires that 'with respect to attacks', a number of precautions should be taken. There are many more Articles that use the term 'attack' when restricting the rights of belligerents.[60]

Thus, the first argument revolves around the question whether the rules on the conduct of hostilities are limited to those acts of hostilities that constitute attacks (as defined in Article 49 of Additional Protocol I) or whether they apply to a broader range of military operations. Broadly speaking, three views have been put forward.

Most commentators are of the opinion that the structure and wording of Additional Protocol I show that, while Article 48 provides a general principle of protection of the civilian population, this general principle is 'operationalized' in the subsequent articles. Only those cyber operations that constitute attacks are subject to the principles of distinction, proportionality, and precaution.[61] An argument made by Michael Schmitt in this regard is that some military operations can be intentionally directed against civilians, for instance psychological operations – which in his view shows that not all military operations are subject to the principle of distinction.[62]

Nils Melzer considers that the debate on the concept of attack does not provide a satisfactory answer to the question because the rules on the conduct of hostilities do not only apply to attacks strictly speaking, but to other operations, too. In his view:

> accurately understood, the applicability of the restraints imposed by IHL on the conduct of hostilities to cyber operations depends not on whether the operations in question qualify as 'attacks' (that is, the predominant form of

60 See, *e.g.*, AP I, Arts 12, 54–56.

61 M. N. Schmitt, 'Cyber operations and the *jus in bello*: key issues', in *Naval War College International Law Studies*, Vol. 87, 2011, p. 91; Robin Geiss and Henning Lahmann, 'Cyber warfare: applying the principle of distinction in an interconnected space', in *Israeli Law Review*, Vol. 45, No. 3, November 2012, p. 2.

62 M. N. Schmitt, *ibid*., p. 91.

> conducting hostilities), but on whether they constitute part of 'hostilities' within the meaning of IHL.[63]

His view is that cyber operations that are designed to harm the adversary, either by directly causing death, injury, or destruction or by directly adversely affecting military operations or military capacity, must be regarded as hostilities.[64] For instance, cyber operations aiming to disrupt or incapacitate an enemy's computer-controlled radar or weapons systems, logistic supply, or communication networks would qualify as hostilities even if they do not cause physical damage. However, cyber operations conducted for the general purpose of intelligence gathering would not fall under hostilities. As far as the non-destructive incapacitation of civilian objects is concerned, Melzer does not come to a definite conclusion but points to the dilemma between adopting a too restrictive or a too permissive interpretation of the law.[65]

Melzer's argument is attractive in that it gives effect to the very object and purpose of the rules on the conduct of hostilities, which is that 'innocent civilians must be kept outside hostilities as far as possible and enjoy general protection against danger arising from hostilities'.[66] However, it leaves open the most critical question, namely whether operations that disrupt civilian infrastructure without destroying it fall under the concept of hostilities.

Heather Harrison Dinniss argues that the prohibition of targeting civilians and civilian objects is not limited to attacks.[67] Rather, she points to the wording of Article 48 of Additional Protocol I and the first sentences of Articles 51 and 57 to argue that the civilian population must be protected not only against attacks, but also more generally against the effects of military operations. Thus, she submits that the principles of distinction, proportionality, and precaution also apply to computer network attacks that fall within the definition of a military operation. To fall within the definition, 'the computer network attack must be associated with the use of physical force, but it does not have to result in violent consequences itself'.[68]

Despite these arguments in favour of expanding the types of operations to which the rules on the conduct of hostilities must apply, it is clear that states did differentiate in Additional Protocol I between the general principles in the respective chapeaux of the rules of distinction and precaution and the specific rules relating to attacks, and that they found it necessary to define attacks specifically in Article 49 of the Protocol. It is difficult to depart from this dichotomy between military operations and attacks.

Nonetheless, Dinniss's argument makes sense of the fact that Articles 48, 51, and 57 contain general clauses that impose limitations for military operations

63 N. Melzer, above note 42.
64 *Ibid.*, p. 28.
65 *Ibid.*
66 Y. Sandoz, C. Swinarski and B. Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, ICRC/Martinus Nijhoff Publishers, Dordrecht, 1987, para. 1923 (hereinafter *Commentary on the Additional Protocols*).
67 H. H. Dinniss, above note 42, pp. 196–202.
68 *Ibid.*, p. 201.

and not only attacks and the content of which would otherwise be difficult to explain. A systematic interpretation of these clauses means that the chapeaux have a meaningful content and are not superfluous. Also, the argument made by Michael Schmitt that some operations, such as psychological operations, can be directed at civilians, implying that some *military* operations could be directed at civilians, rests on a misunderstanding of the concept of military operations. Indeed, while it is true that some cyber operations, such as psychological operations, can be directed at the civilian population, this is because they do not fall under military operations or hostilities within the meaning intended by the Protocol's drafters. According to the ICRC Commentary, the term 'operations' in Article 48 means military operations and refers to 'all movements and acts related to hostilities that are undertaken by armed forces'.[69] The term 'military operations' in Article 51 is described as 'all the movements and activities carried out by armed forces related to hostilities'.[70] And in Article 57 it 'should be understood to mean any movements, manoeuvres and other activities whatsoever carried out by the armed forces with a view to combat'.[71] In other words, operations such as propaganda, espionage, or psychological operations will not fall under the concepts of hostilities or military operations and are therefore not governed by the principles of distinction, proportionality, and precaution, even if they are carried out by the armed forces.

Thus, while some of the more specific content of Articles 51 and 57 of Additional Protocol I might address the specificities of attacks, there is a good argument that other military operations cannot be entirely exempt from the obligations of distinction, proportionality, and precaution, since Article 48 and the chapeaux of Articles 51 and 57 would otherwise be superfluous. However, since there is disagreement about this question it is prudent to nonetheless have a closer look at the definition of 'attack' and what types of cyber operation fall under it. Indeed, most of the cyber operations in the examples mentioned above fall under the concept of attack and would be prohibited if targeted at civilian infrastructure. Thus, it will be shown that in most of the examples given above the operations amount to attacks, and hence the question whether only 'attacks' or also 'hostilities' or 'military operations' are subject to the rules on the conduct of hostilities is moot.

What is an attack?

As said above, operations in cyber space differ from traditional warfare in that the means and methods of attack do not entail traditional kinetic force, or what is commonly understood as violence. Yet, attacks are defined in Article 49(1) of Additional Protocol I (which reflects customary IHL) as 'acts of violence against the

69 *Commentary on the Additional Protocols*, above note 68, para. 1875.
70 *Ibid.*, para. 1936.
71 *Ibid.*, para. 2191.

adversary, whether in offence or in defence'. In the mind of the drafters, this connoted physical violence.

First, it should be recalled that, based on the fact that an attack must be an act of violence, there is broad agreement nowadays that violence does not refer to the means of the attack – which would only encompass kinetic means.[72] Military operations that result in violent consequences constitute attacks. For instance, it is uncontroversial that the use of biological, chemical, or radiological agents would constitute an attack, even though the attack does not involve physical force.[73] Therefore, it has been accepted for a long time that what defines an attack is not the violence of the means, but the violence of the consequences.[74] Thus, even a data stream passed through cables or satellite could fall under the concept of attack.

The controversy lies on the side of the effects of cyber operations. It turns on those operations that do not cause death or injury to persons or physical destruction or damage to objects as kinetic operations would, but rather disrupt the functioning of objects without causing them physical damage – such as in the examples given above. As these examples show, the consequences of cyber operations do not necessarily have violent effects in that they do not cause physical damage or destruction. In the examples given above the consequences in the physical realm would be at the most indirect: for instance, if the electrical grid is shut down, this may lead to power outages for vital services such as hospitals. In some cases the consequences are limited to the ability to communicate or engage in commercial activities, such as when a banking system is disrupted. Can such operations be considered attacks within the meaning of Article 49 of Additional Protocol I?

Two positions have been put forward with respect to this question. According to Michael Schmitt's earlier writings:

> [a] cyber operation, like any other operation, is an attack when resulting in death or injury of individuals, whether civilians or combatants, or damage to or destruction of objects, whether military objectives or civilian objects.[75]

Damage, in this view, only refers to physical damage. Computer network attacks that cause mere inconvenience, or merely temporarily interrupt the functioning of objects, do not constitute attacks unless they cause human suffering. Critically, the mere disruption of the functionality of an object, short of leading to such human

72 Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge University Press, Cambridge, 2004, p. 84; M. N. Schmitt, above note 61, p. 5.

73 ICTY, *Prosecutor* v. *Dusko Tadić*, Decision on the Defence Motion for Interlocutory Appeal, 2 October 1995, paras. 120 and 124 (regarding chemical weapons); *Tallinn Manual*, above note 27, Commentary on Rule 30, para. 3; Emily Haslam, 'Information warfare: technological changes and international law', in *Journal of Conflict and Security Law*, Vol. 5, No. 2, 2000, p. 170.

74 Michael N. Schmitt, 'Wired warfare: computer network attack and *jus in bello*', in *International Review of the Red Cross*, Vol. 84, No. 846, June 2002, p. 377; *Tallinn Manual*, above note 27, Commentary on Rule 30, para. 3.

75 M. N. Schmitt, above note 61, p. 6.

suffering or short of resulting in physical damage or the complete and permanent loss of functionality of the targeted object, does not amount to an attack.[76]

According to Knut Dörmann, cyber operations can also constitute attacks even if they do not lead to the destruction of the object. This view is predicated on the definition of a military objective in Article 52(2) of Additional Protocol I, which states that a military objective is one '... whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage'. From the term 'neutralization' it can be seen that '[i]t is irrelevant whether an object is disabled through destruction or in any other way'.[77] Critics answer that the definition of military objectives is not entirely on point because it presupposes an attack in the first place and does not define the attack in itself.[78] This criticism fails to acknowledge that 'neutralization' was meant to encompass 'an attack for the purpose of denying the use of an object to the enemy without necessarily destroying it'.[79] This shows that the drafters had in mind not only attacks that are aimed at destroying or damaging objects, but also attacks for the purpose of denying the use of an object to the enemy without necessarily destroying it. So, for instance, an enemy's air defence system could be neutralized through a cyber operation for a certain duration by interfering with its computer system but without necessarily destroying or damaging its physical infrastructure.[80]

More recently, the Tallinn Manual defines a cyber attack as 'a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[81] However, as the commentary shows, experts disagreed as to what exactly was to be understood as 'damage' to objects, and whether or what type of impairment of the functioning of an object would fall within its definition.[82]

The weakness of the first opinion is that it is under-inclusive. First, it would not make sense to consider that if a civilian object is rendered useless, regardless of the way in which this was done, it is not damaged. Whether an electrical grid is put out of order by physical damage or interference with the computer system by which it is run cannot be a relevant criterion. A contrary opinion would lead to the conclusion that the destruction of one house by bombing would be an attack, but the

76 Michael Schmitt now takes a somewhat different position and argues that '[d]estruction includes operations that, while not causing physical damage, nevertheless "break" an object, rendering it inoperable, as in the case of a cyber operation that causes a computer-reliant system to no longer function unless repaired'; '"Attack" as a term of art in international law: the cyber operations context', in *2012 4th International Conference on Cyber Conflict*, C. Czosseck, R. Ottis and K. Ziolkowski (eds), 2012, NATO CCD COE Publications, Tallinn, p. 291; see also M. N. Schmitt, above note 28, p. 252.

77 K. Dörmann, above note 42, p. 4.

78 M. N. Schmitt, above note 61, p. 8.

79 Michael Bothe, Karl Josef Partsch and Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary to the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, Martinus Nijhoff Publishers, Dordrecht, 1982, p. 325.

80 This was reportedly done in the September 2007 Israeli air attack on a Syrian structure believed to be housing a nuclear-weapons development programme. Israel had hacked into the Syrian air defences and controlled them during the attack; see 'Arab & Israeli cyber-war', in *Day Press News*, 22 September 2009, available at: http://www.dp-news.com/en/detail.aspx?articleid=55075.

81 *Tallinn Manual*, above note 27, Rule 30.

82 *Ibid.*, Commentary on Rule 30, paras 10–12.

disruption of an electrical grid supplying thousands or millions of people would not. Second, reference to the principle of proportionality gives an indication of the incidental effects against which the rules on the conduct of hostilities mean to protect civilians, namely excessive 'incidental loss of civilian life, injury to civilians, damage to civilian objects'. 'Damage' is different from 'destruction'. It means 'harm . . . impairing the value or usefulness of something . . .'.[83] Thus, disrupting the functioning of certain systems by interfering with their underlying computer systems can amount to damage insofar as it impairs their usefulness. Third, the view that there must be complete and permanent loss of functionality without physical damage does not make sense in information technology. Since data can always be restored or changed there is no permanent and complete loss of functionality of an object short of physical damage. Thus, an attack must also be understood to encompass such operations that disrupt the functioning of objects without physical damage or destruction, even if the disruption is temporary.

Yet, an overly broad interpretation of the term 'attack' would mean that all interferences with civilian computer systems would amount to attacks: the interruption of email or social network communications, of online booking or shopping systems, etc. To equate such disruptions of what are essentially communication systems with attacks would probably go beyond the scope of what was envisaged by the rules on the conduct of hostilities. These rules have traditionally sought to prevent damage to civilian infrastructure that manifests itself in the physical world, not interference with propaganda, communication, or economic life. In today's world, the reliance of civilian life on communication systems blurs these lines, and it is not easy to distinguish between what is 'mere' communication and what goes beyond.

Existing IHL norms and their object and purpose provide a number of indications for distinguishing between operations that amount to attacks and those that do not. First, as said above, the concept of 'attacks' does not include dissemination of propaganda, embargoes, or other non-physical means of psychological or economic warfare.[84] Cyber operations that are equivalent to espionage, to the dissemination of propaganda, to embargoes, or other non-physical means of psychological or economic warfare will not fall under the definition of 'attacks'.

Second, IHL does not prohibit blockades or economic sanctions that deliberately target not only the military but also the civilian population and economy. Thus, the term 'attack' cannot comprise cyber operations that would be tantamount to economic sanctions. This is not to say that such operations would not have limits under IHL (such as the prohibition of destroying, removing, or rendering useless objects indispensable to the survival of the civilian population or obligations with respect to the passage of humanitarian relief), but, since they do not constitute attacks, there is no prohibition under IHL against directing them at civilians.

83 *Concise Oxford Dictionary.*
84 M. Bothe *et al.*, above note 79, p. 289.

Third, the rules on the conduct of hostilities do not intend to prohibit all operations that interfere with civilian communication systems. For instance, not all denial of service operations,[85] such as blocking a television broadcast or a university website, would amount to an attack. Mere interference with propaganda, for instance, will probably also not constitute an attack. The parallel of such operations in the physical world is probably the jamming of radio communications or television broadcasts – which is not considered an attack in the sense of IHL.

To differentiate between those operations that amount to attacks and those that do not, the criterion of inconvenience is sometimes put forward.[86] The argument is inconvenience, such as rationing of food, need not be taken into account for 'incidental civilian damage'. Therefore, something that causes mere inconvenience cannot amount to and attack. While the criterion of inconvenience is not without its merits, there might be disagreement on what represents inconvenience in terms of interferences with cyber technology and communication. For instance, while it might be possible to agree that the interruption of an online booking system causes mere inconvenience, consensus might be more difficult to achieve around issues such as interference with banking services. It remains to be seen how these interferences will be considered in the future, in particular in state practice.

Summary

In sum, a cyber operation can constitute an attack within the meaning of IHL when it causes death or injury or physical destruction or damage, but also if it interferes with the functioning of an object by disrupting the underlying computer system. Thus, if an air defence system is put out of order by a cyber operation, if a cyber operation disrupts the functioning of an electrical grid, or if the banking system is disabled, this amounts to an attack. However, not all cyber operations directed at disrupting the functioning of infrastructure amount to attacks. Where the operation is not directed at the physical infrastructure relying on the computer system, but essentially at blocking communication, it is more akin to jamming radio signals or television broadcasts – unless it is, of course, part of an attack, such as blocking an air defence system. The difference lies in the fact that in some cases it is the communication function of cyber space alone that is being targeted; in other cases, it is the functioning of the object beyond cyber space in the physical world. While interference with cyber systems that leads to disruption in the physical world constitutes attacks, the question of

85 That is, cyber operations that make the targeted computer's service unavailable to the usual users or customers.

86 M. N. Schmitt, above note 74, p. 377; Program on Humanitarian Policy and Conflict Research at Harvard University, *Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare,* 2010, Commentary on Article 1(d), para. 7, available at: http://www.ihlresearch.org/amw/aboutmanual.php (hereinafter *Commentary on HPCR Manual on Air and Missile Warfare*); Michael N. Schmitt, 'Cyber operations in international law: the use of force, collective security, self-defense and armed conflict', in National Research Council, *Proceedings of a Workshop on Deterring Cyber Attacks*, Washington, DC, The National Academies Press, 2010, p. 155.

interference with communication systems such as email systems or the media is not entirely solved.

The principle of distinction

The principle of distinction requires that parties to a conflict distinguish at all times between civilians and combatants and between civilian objects and military objectives.[87] It is, in the words of the ICJ, a cardinal principle of IHL.[88] Attacks may only be directed against combatants or military objectives. This means that, in planning and carrying out cyber operations, the only targets permissible under IHL are military objectives, such as computers or computer systems that make an effective contribution to concrete military operations. Attacks via cyber space may not be directed against computer systems used in purely civilian installations.

Some of the discussion around military objectives in cyber space is a cause for concern from the point of view of the protection of the civilian population. Indeed, it appears that cyber operations might be particularly well suited to target certain civilian objects, because they enable the belligerents to reach some targets that might have been less reachable previously, such as financial networks or medical data networks.[89] Some have argued that cyber warfare might lead to a sort of 'expanded target list'[90] compared to traditional warfare. Also, because cyber operations can disable an object's functioning without causing physical damage, some commentators have argued that the use of cyber operations expands the range of legitimate targets because it enables attacks with reversible effects against objects that it would otherwise be prohibited to attack.[91] It has also been argued that:

> [t]he potentially non-lethal nature of cyber weapons may cloud the assessment of an attack's legality, leading to more frequent violations of the principle of distinction in this new form of warfare than in conventional warfare.[92]

Against this background, it is important to recall the rules of IHL governing attacks on objects and to address a number of specific legal problems that might arise through the use of computer network attacks.

87 AP I, Arts 48, 51 and 52; Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law, Vol. I, Rules*, (hereinafter 'Study on customary international humanitarian law'), ICRC and Cambridge University Press, 2005, Rules 1–10.

88 ICJ, *Legality of the Threat of Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996, para. 78.

89 Michael N. Schmitt, 'Ethics and military force: the *jus in bello*', Carnegie Council for Ethics in International Affairs, 7 January 2002, available at: http://www.carnegiecouncil.org/studio/multimedia/20020107/index.html.

90 This is the expression used by Eric Talbot Jensen, 'Unexpected consequences from knock-on effects: a different standard for computer network operations?', in *American University International Law Review*, Vol. 18, 2002–2003, p. 1149.

91 Mark R. Shulman, 'Discrimination in the law of information warfare', in *Columbia Journal of Transnational Law*, 1999, pp. 963 *ff*.

92 Jeffrey T. G. Kelsey, 'Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare', in *Michigan Law Review*, Vol. 106, 2007–2008, p. 1439.

Under IHL, civilian objects are all objects that are not military objectives.[93] Military objectives are defined in Article 52(2) of Additional Protocol I as:

> those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.

According to Article 52(3) of Additional Protocol I, objects that are normally dedicated to civilian purposes shall be presumed not to be used to make an effective contribution to military action. So, for instance, if some particularly sensitive civilian infrastructure, such as most chemical plants, relies on a closed computer network, this network must be presumed to be civilian.

As the wording of Article 52(2) makes clear, there must be a close nexus between the potential target and military action. The term 'military action' denotes the enemy's war-fighting capabilities. This nexus is established through the four criteria of nature, location, purpose, and use. Nature refers to the intrinsic character of an object, such as a weapon. Objects that are not military in nature may also make an effective contribution to military action by virtue of their particular location, their purpose, or their present use.

In this respect, four issues in particular should be highlighted that can have potentially serious implications for civilian infrastructure: most importantly, the fact that most international cyber infrastructure is in practice so-called dual-use infrastructure; the question whether factories producing hardware and software used by the military become military objectives; the targeting of objects with so-called war-sustaining capability; and the legal consequences of the social media networks being used for military purposes, such as information on targets.

Dual-use objects in cyberspace

So-called dual-use objects – a term not found as such in IHL provisions – are those that are used for both civilian and military purposes. Due to their use for military purposes, they become military objectives under Article 52(2) of Additional Protocol I and legitimate targets of attack. Examples frequently given are parts of the civilian infrastructure that supply the military for their operations, such as power plants or electrical grids.

According to today's prevailing view, an object cannot be a civilian and a military object at the same time. The moment it is used for military action it becomes a military objective in its entirety (except if separable parts remain civilian – for instance, different buildings of a hospital).[94] As opposed to the ICRC's 1956 proposal, which, outside purely military material and installations, mentioned

93 AP I, Art. 52(1), reflective of customary international law; *Study on customary international humanitarian law,* above note 87, Rule 9.

94 *The Commander's Handbook on the Law of Naval Operations*, Department of the Navy/Department of Homeland Security, USA, July 2007, para. 8.3; *Tallinn Manual*, above note 27, Commentary on Rule 39, para 1.

civilian communication, transport, or industry 'of fundamental military importance' or 'fundamental importance for the conduct of the war',[95] it is generally considered today that the object becomes a military objective even if its military use is only marginal compared to its civilian use. For instance, if a plant provides a small percentage of fuel used in military operations, even if this is not its main purpose, it becomes a military objective.

The dangers in cyber space are evident: virtually the entire international cyber infrastructure – that is, computers, routers, cables, and satellites – is used for both civilian and military communications.[96] An undersea cable that transports military communications becomes a military objective – with the consequence that (subject to other rules of IHL, namely proportionality) it can not only be the subject of a cyber operation to interrupt the military communication, it could also be destroyed. Similarly, a server containing 5 per cent military data would become a legitimate target. This is particularly important to bear in mind in an era of increased cloud computing, where the users of cloud computing are typically not aware on what servers their data are being stored and what other data are stored on that server. It is reported that approximately 98 per cent of US government communications use civilian-owned and -operated networks.[97]

The danger that any part of the cyber infrastructure could be targeted is very real. Indeed, while in certain circumstances states might seek to disable very specific functions of the adversary's military infrastructure, the fact that all of cyber space is used for military operations means that in any armed conflict it will be of important strategic interest to degrade the adversary's communication networks and access to cyber space. This will mean denying the adversary access to critical routes in cyber space, degrading its main routers or access to major communication nodes, not just targeting specific computer systems of the military infrastructure.[98] Unlike in the naturally occurring theatres of war, such as land or airspace, the man-made theatre of cyber space means that the

95 In the ICRC's Draft Rules for the Limitation of Danger incurred by the Civilian Population in Time of War, the list drawn up by the organization with the help of military experts and presented as a model, subject to modification, was as follows: 'I. The objectives belonging to the following categories are those considered to be of generally recognized military importance: . . . (6) *Those* of the lines and means of communication (railway lines, roads, bridges, tunnels and canals) which are of *fundamental military importance*; (7) The installations of broadcasting and television stations; telephone and telegraph exchanges of *fundamental military importance*; (8) Industries of fundamental importance for the conduct of the war: (a) industries for the manufacture of armaments . . .; (b) industries for the manufacture of supplies and material of a military character . . .; (c) factories or plant constituting *other* production and manufacturing centres of fundamental importance for the conduct of war, such as the metallurgical, engineering and chemical industries, *whose nature or purpose is essentially military*; (d) storage and transport installations whose basic function it is to serve the industries referred to in (a)–(c); (e) installations providing energy *mainly for national defence*, e.g., coal, other fuels, or atomic energy, and plants producing gas or electricity mainly for military consumption.' (emphasis added). See *Draft Rules for the Limitation of the Dangers incurred by the Civilian Population in Time of War*, ICRC, 1956, available at: http://www.icrc.org/ihl/INTRO/420?OpenDocument.

96 See also R. Geiss and H. Lahmann, above note 61, p. 3.

97 Eric Talbot Jensen, 'Cyber warfare and precautions against the effects of attacks', in *Texas Law Review*, Vol. 88, 2010, p. 1534.

98 US Department of Defense, *Quadrennial Defence Review Report*, February 2010, pp. 37–38, available at: http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf.

belligerents will not only focus on the travelling weapon but on the routes themselves.[99] For instance, in airspace, only the aircraft qualifies as a military objective; in cyber warfare, however, the physical infrastructures through which the cyber weapons (malicious codes) travel qualify as military objectives.

The humanitarian consequences of this situation are of utmost concern for the protection of the civilian population. In a world in which a large part of civilian infrastructure, civilian communication, finance, economy, and trade rely on international cyber infrastructure it becomes all too easy for parties to conflicts to destroy this infrastructure. There is no need to argue that a banking network is used for military action, or that an electrical grid is dual use. Disabling the major cables, nodes, routers, or satellites that these systems rely on will almost always be justifiable by the fact that these routes are used to transmit military information and therefore qualify as military objectives.

The Tallinn Manual states:

> the circumstances under which the Internet in its entirety could be attacked [are] so highly unlikely as to render the possibility purely theoretical at the present time. Instead, the International Group of Experts agreed that, as a legal and practical matter, virtually any attack against the Internet would have to be limited to certain discrete segments thereof.[100]

It also mentions the principles of precaution and proportionality, which would have to be respected if the Internet or large portions thereof were targeted. However, while this might seem reassuring at first sight, it leaves the problem that whether or not the Internet in its entirety can be targeted, any of its segments can be targeted if used for military communication and its destruction or neutralization offers a definite military advantage (again subject to proportionality and precautions).

Furthermore, cyber space is resilient in the sense that if information cannot flow through one channel there are multiple routes and alternatives and the information can usually be transmitted through another path. As the Tallinn Manual states:

> Cyber operations pose unique challenges in this regard. Consider a network that is being used for both military and civilian purposes. It may be impossible to know over which part of the network military transmissions, as distinct from civilian ones, will pass. In such cases, the entire network (or at least those aspects in which transmission is reasonably likely) qualifies as a military objective.[101]

The consequence of this would be that in some circumstances virtually all parts of the Internet might qualify as a military objective because they are all possible routes for the transmission of military information.

99 R. Geiss and H. Lahmann, above note 61, p. 9.
100 *Tallinn Manual*, above note 27, Commentary on Rule 39, para 5.
101 *Ibid.*, Commentary on Rule 39, para 3.

The prevailing wide interpretation of dual-use objects as military objectives is already not without its problems in the physical world.[102] In cyber space the consequences could be exacerbated to an extreme point where nothing civilian remains and the basic rule that the civilian population shall enjoy general protection against dangers arising from military operations becomes virtually empty of content, subject only to the principles of proportionality and precaution.

Lastly, if most of the cyber infrastructure around the world is of a dual-use nature and could be considered a military objective, this raises the fundamental question of the geographical limits of the armed conflict. There are truly no borders in cyber space, and computer systems from anywhere can be (remotely) attacked, manipulated, or transformed into means of warfare and military objectives. It must be borne in mind that the consequence would not only be that such computers could be counter-hacked by the targeted computer systems. In theory, as military objectives they could be destroyed through kinetic means. For instance, a botnet could be used to launch an attack destroying an adversary's cyber infrastructure. To conduct such an operation, the party to the conflict launching the attack would remotely control thousands or millions of computers around the world, which would transmit the malware to the target computers. If such a botnet were to lead to all of the millions of computers that it uses throughout the world being defined as military objectives liable to attack, the result would be a sort of total cyber war. The logical consequence, that all these computers around the world become military targets, would be contrary to the foundations of the law of neutrality in international armed conflicts (and mainly with its underlying rationale, which is to spare the third country and its inhabitants from the effects of hostilities) or with the geographical limitations of the battlefield in non-international armed conflicts.[103] In an international armed conflict the law of neutrality would put certain limits on the right of the attacked state to defend itself by attacking infrastructure in neutral territory.[104] First, the attacked state must notify the neutral state and give it a reasonable time to terminate the violation; second, the attacked state is allowed to take measures to terminate the violation of neutrality only if that violation

102 See also Marco Sassòli, 'Legitimate targets of attacks under international humanitarian law', Background Paper prepared for the Informal High-Level Expert Meeting on the Reaffirmation and Development of International Humanitarian Law, Cambridge, 27–29 January 2003, HPCR, 2003, pp. 3–6, available at: http://www.hpcrresearch.org/sites/default/files/publications/Session1.pdf; William M. Arkin, 'Cyber warfare and the environment', in *Vermont Law Review*, Vol. 25, 2001, p. 780, describing the effects in 1991 of the air attacks on Iraqi electrical power on not only the civilian electricity supply, but also water distribution, purification, sewage, and the health infrastructure; R. Geiss and H. Lahmann, above note 61, p. 16.

103 The boundaries of the battlefield of non-international armed conflict are a matter of dispute and would go far beyond the scope of this article – but the difficulties raised by cyber warfare seem almost unanswerable in this respect. For the ICRC's view, see ICRC, *Report on International Humanitarian Law and the challenges of contemporary armed conflicts*, 31st International Conference of the Red Cross and Red Crescent, Geneva, 28 November–1 December 2011, Report prepared by the ICRC, October 2011, pp. 21–22; for a discussion of the geographical implications in cyber warfare, see the *Tallinn Manual*, above note 27, Commentary on Rule 21.

104 These are derived from Article 22 of the San Remo Manual on International Law Applicable to Armed Conflicts at Sea, of 12 June 1994, available at: http://www.icrc.org/IHL.nsf/52d68d14de6160e0c12563da005fdb1b/7694fe2016f347e1c125641f002d49ce!OpenDocument.

constitutes a serious and immediate threat to its security and only if no other feasible and timely alternative exists to respond to the threat. These restrictions are relatively broad, and in order to be truly protective for the civilian population of the neutral state they would presumably have to be narrowly interpreted. In non-international armed conflicts the law of neutrality is not applicable. However, it would completely break open the geographical limits of the battlefield of non-international armed conflicts to consider that the armed conflict takes place anywhere where a computer, cable, or node is used for military action (and would therefore normally constitute a military objective).

In sum, it becomes clear that, in cyber space, the principle of distinction appears to hold little promise for the protection of civilian cyber infrastructure and all the civilian infrastructure that relies on it. In such situations the main legal protection for civilian infrastructure will be the principle of proportionality – which will be addressed below.[105]

The problem that, in cyber space, most infrastructure is dual use is certainly the most important concern and other legal issues appear less pressing. Some of them will nonetheless be addressed in the following paragraphs.

Corporations that produce information technology used for military action

Since hardware and software are used for much military machinery, information technology (IT) corporations that produce them could be seen as 'war-supporting military objectives'[106] – in parallel with munitions factories. This would likely mean that a number of IT corporations around the world would constitute legitimate targets as many of them probably provide some IT infrastructure for the military.[107] Eric Talbot Jensen, for instance, asks whether the Microsoft Corporation would constitute a legitimate target 'based on the support it provides to the U.S. war effort by facilitating U.S. military operations'. In his view, '[t]he fact that the corporation and its headquarters provide a product that the military finds essential to function, as well as customer service to support that product, may provide sufficient facts to conclude that it is a dual use target', but he doubts whether a definite military advantage would accrue from such an attack.[108]

The example shows that the parallel with munitions factories should not be overstretched. The relevant criterion of Article 52(2) of Additional Protocol I is that the object must by its use make an effective contribution to military action.

105 *Commentary on HPCR Manual on Air and Missile Warfare*, above note 86, Commentary on Rule 22(d), para. 7; *Tallinn Manual*, above note 27, Commentary on Rule 39, para. 2; E. T. Jensen, above note 90, p. 1157.

106 M. N. Schmitt, above note 61, pp. 8 *ff*.

107 It is reported that the US Department of Defense will host contractors who want to propose new technologies for cyber warfare: S. Shane, above note 3.

108 E. T. Jensen, above note 90, pp. 1160 and 1168; see also E. T. Jensen, above note 97, p. 1544: 'If a civilian computer company produces, maintains, or supports government cyber systems, it seems clear that an enemy could determine that company meets the test of Article 52 and is targetable'.

First, corporations as such are not physical objects, but legal entities, and so the question would instead be whether any of their locations (that is, buildings) have become military objectives. Second, there is a difference between weapons and IT tools. Weapons are by their nature military objectives, which generic IT systems are not. Thus, one might have to differentiate between factories that actually develop what might be called cyber weapons, that is specific codes/protocols that will be used for a specific computer network attack (so, for instance, the location where a specific virus like Stuxnet is being developed), and those that just provide the military with generic IT supplies, which are not so different from, say, food supplies.[109]

War-fighting capability or war-sustaining capability?

In cyber warfare, where the temptation to target civilian infrastructure is possibly higher than in traditional warfare, it is important to keep in mind that for a civilian object to become a military objective its contribution to military action must be directed towards the actual war-fighting capabilities of a party to the conflict. If an object merely contributes to the war-sustaining capability of a party to the conflict (its general war effort), it does not qualify as a military objective.

In the US *Commander's Handbook on the Law of Naval Operations*, the expression 'makes an effective contribution to military action' from Article 52(2) of Additional Protocol I has been widened and replaced by 'effectively contribute to the enemy's war-fighting or war-sustaining capability'.[110] This position is mainly geared towards economic targets, which may indirectly support or sustain the enemy's military capability.[111] A 1999 assessment of the law by the US Department of Defense's Legal Counsel in respect of cyber operations states:

> purely civilian infrastructures must not be attacked unless the attacking force can demonstrate that a definite military advantage is expected from the attack. . . . In a long and protracted armed conflict, damage to the enemy's economy and research and development capabilities may well undermine its war effort, but in a short and limited conflict it may be hard to articulate any expected military advantage from attacking economic targets.[112]

109 The *Tallinn Manual* also fails to come to a definite conclusion on this question: 'The difficult case involves a factory that produces items that are not specifically intended for the military, but which nevertheless are frequently put to military use. Although all of the Experts agreed that the issue of whether such a factory qualifies as a military objective by use depends on the scale, scope, and importance of the military acquisitions, the Group was unable to arrive at any definitive conclusion as to the precise thresholds.'

110 *The Commander's Handbook on the Law of Naval Operations*, above note 94, para. 8.2.

111 M. N. Schmitt, 'Fault lines in the law of attack', in S. Breau and A. Jachec-Neale (eds), *Testing the Boundaries of International Humanitarian Law*, British Institute of International and Comparative Law, London, 2006, pp. 277–307. For the underlying rationale of such an approach, see, for instance, Charles J. Dunlap, 'The end of innocence, rethinking noncombatancy in the post-Kosovo era', in *Strategic Review*, Vol. 28, Summer 2000, p. 9; Jeanne M. Meyer, 'Tearing down the façade: a critical look at current law on targeting the will of the enemy and Air Force doctrine', in *Air Force Law Review*, Vol. 51, 2001, p. 143; see J. T. G. Kelsey, above note 92, p. 1447, who advocates a new definition of military objectives in order to include certain civilian infrastructure and services.

112 Department of Defense Office of General Counsel, *An Assessment of International Legal Issues in Information Operations*, May 1999, p. 7, available at: http://www.au.af.mil/au/awc/awcgate/dod-io-legal/

These approaches overlook the legal restrictions imposed by IHL. Damage to the enemy's civilian economy, research, and development capabilities in themselves is never allowed under IHL, regardless of the perceived military advantage, and regardless of the duration of the conflict. Otherwise, there would be no limits to warfare as virtually the entire economy of a country can be considered to be war-sustaining.[113] It is particularly important to recall this in the context of cyber warfare and to point to the potentially devastating consequences of a broad definition of military objectives for the civilian population.

The media and social networks

The Tallinn Manual addresses the thorny question of social networks being used for military purposes:[114]

> Recent conflicts have highlighted the use of social networks for military purposes. For example, Facebook has been used for the organization of armed resistance operations and Twitter for the transmission of information of military value. Three cautionary notes are necessary. First, it must be remembered that this Rule [that an object used for both civilian and military purposes is a military objective] is without prejudice to the rule of proportionality and the requirement to take precautions in attack … Second, the issue of the legality of cyber operations against social networks depends on whether such operations rise to the level of an attack. If the operations do not, the issue of qualification as a military objective is moot … Third, this does not mean that Facebook or Twitter as such may be targeted; only those components thereof used for military purposes may be attacked [so long as the attack complies with other requirements of the law of armed conflict].[115]

The qualification of social networks such as Facebook or Twitter as military objectives would pose a number of problems. Indeed such networks contain such vast amounts of data – most of which is entirely unrelated to the specific information that would need to be targeted – that it would appear to be difficult to

dod-io-legal.pdf. The position of the United States in the latest Report of the Secretary-General is ambiguous at best when it states that the principles of *jus in bello* 'prohibit attacks on purely civilian infrastructure, the disruption or destruction of which would produce no meaningful military advantage'. If this is meant to imply that attacks on purely civilian infrastructure would not be allowed if the destruction or disruption would produce a meaningful military advantage, it would be incompatible with IHL, which never allows attacks on purely civilian objects (Report of the Secretary-General, 15 July 2011, UN Doc. A/66/152, p. 19).

113 M. Sassòli, above note 102; Stephan Oeter, 'Means and methods of combat', in Dieter Fleck (ed.), *The Handbook of Humanitarian Law in Armed Conflicts*, Oxford University Press, Oxford, 1995, para. 442.5.

114 It has been reported, for instance, that NATO acknowledged that social media such as Twitter, Facebook, and YouTube contributed to their targeting process in Libya, after being checked against other sources: Graeme Smith, 'How social media users are helping NATO fight Gadhafi in Libya', in *The Globe and Mail*, 14 June 2011; Tim Bradshaw and James Blitz, 'NATO draws on Twitter for Libya strikes', in *The Washington Post*, 16 June 2011.

115 *Tallinn Manual*, above note 27, p. 114.

qualify any such network as one military objective. A further question would be whether it is technically possible to only attack those components that are used for military purposes among the unstructured data of such networks.

An equally difficult question arises with respect to the media. The Tallinn Manual states:

> An interesting case involves media reports. If such reports effectively contribute to the enemy's operational picture, depriving the enemy of them might offer a definite military advantage. Some members of the International Group of Experts took the position that cyber infrastructure supporting their transmission qualifies as a military objective, although they cautioned that the infrastructure could only be attacked subject to the Rules regarding attack, especially those on proportionality … and precautions in attack … In particular, they noted that the latter requirement would usually result in a requirement to only mount cyber operations designed to block the broadcasts in question. Other Experts argued that the nexus between the cyber infrastructure's contribution to military action was too remote to qualify the infrastructure as a military objective. All members of the International Group of Experts agreed that such assessments are necessarily very contextual.[116]

Even if a particular report would make an effective contribution to military action, this should not lead to the conclusion that either the media corporation responsible or the cyber infrastructure transmitting it can be the subject of attack. As far as media corporations are concerned, the potential consequences of accepting their targetability would be momentous. Take an international broadcaster like the BBC. First, the expression 'contributing to the enemy's operational picture' is far too broad, is broader than making a direct contribution to the enemy's military action, as required by Article 52(2) of Additional Protocol I. Second, even if the media report contained tactical information, for instance on specific targets, the proposition that the media company could be targeted is highly problematic. Beyond the corporation itself, if all of the cyber infrastructure through which the reports are transmitted were to be considered a military objective, this would mean a large part of the globe's cyber infrastructure – again, as with dual-use objects, bearing in mind that the consequence of considering an object a military objective is that it can also be targeted by kinetic means, implying that the physical location from where and through which the reports are being transmitted – could be damaged or destroyed. Last, as said above, the example of media corporations brings into sharp contrast the problem of the geographical limits of the battlefield. Also, the law of neutrality would impose a number of limits in an international armed conflict on a state's ability to target infrastructure in a neutral state.[117]

116 *Ibid.*, p. 113.
117 See above section '*Dual-use objects in cyberspace*'.

The prohibition of indiscriminate attacks and of indiscriminate means and methods of warfare

Indiscriminate attacks are prohibited.[118] Indiscriminate attacks are those:

- which are not directed at a specific military objective,
- which employ a method or means of combat which cannot be directed at a specific military objective, or
- which employ a method or means of combat the effects of which cannot be limited as required by IHL,

and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction. Parties to a conflict 'must consequently never use weapons that are incapable of distinguishing between civilian and military targets'.[119]

As said above, the fact that most of cyber space can probably be considered dual use is likely to make it difficult to separate military from civilian infrastructure. However, even where military and civilian infrastructure can still be separated and distinguished, another risk is that attacks will be indiscriminate because of the interconnectedness of cyber space.[120] Cyber space consists of innumerable interwoven computer systems across the world. Even if military computer systems are separate from civilian ones they are often interconnected with commercial, civilian systems and rely on them in whole or in part. Thus, it might well be impossible to launch a cyber attack on military infrastructure and limit the attack or its effects to just that military objective. Viruses and worms are examples of methods of computer network attack that could fall into this category if their effects are not limited by their creators. The use of a worm that replicates itself and cannot be controlled, and might therefore cause considerable damage to civilian infrastructure, would be a violation of IHL.[121]

This concern has been dismissed by some commentators as exaggerated, particularly based on the fact that, because most cyber operations would only be efficient if they targeted very specific, highly specialized systems, their effects on other computers would not be damaging. The example given is that of the Stuxnet virus, which was very precisely written to be used against the nuclear installations in the Islamic Republic of Iran.[122]

Indeed, if a virus is introduced into a closed military system or written to prevent its spreading into other systems, there might be no risk for outside civilian infrastructure. But it is quite imaginable that a party to a conflict takes no such precautions or develops cyber weapons that have effects on networks that it might

118 *Study on customary international humanitarian law*, Rule 12; AP I, Art. 51(4).
119 ICJ, above note 88, para. 78.
120 K. Dörmann, above note 42, p. 5.
121 The worm could either not be able to be directed at a specific military objective (cf. *Study on customary international humanitarian law*, Rule 12 (b), AP I, Art. 51(4)(b)) or have effects that cannot be limited as required by IHL (see *Study on customary international humanitarian law*, Rule 12(c), AP I, Art. 51(4)(c)).
122 T. Rid, above note 24.

not have foreseen. The fact that it is possible to design cyber weapons that are not indiscriminate does not mean that there is not a high potential for indiscriminate attacks. Even the Stuxnet virus – as reported in the media – shows how difficult it is to control the effects of viruses; it is reported that this virus was not intended to infect computers outside the targeted systems of the nuclear installations, yet somehow it replicated itself outside Iran.[123] While the spread of the virus far beyond the intentions of its creators might not have caused any damage, it shows how difficult it is to control that spread.

There is therefore a twofold burden on the belligerent parties. First, they may not employ cyber weapons that are indiscriminate by nature, such as viruses or worms that replicate without any possibility of controlling them (in parallel to bacteriological weapons, for instance). The use of such weapons should be outlawed during the review of the weapon when it is being developed or acquired – if it can never be employed without striking military and civilian objectives alike, it is incompatible with IHL requirements.[124] Second, at each attack, the belligerent party has to verify whether, in the particular circumstances of the case, the cyber weapon employed can be and is directed at a military target and whether its effects can be controlled within the meaning of IHL.

The principle of proportionality

Considering the dual-use nature of most cyber infrastructure, on the one hand, and the risk of repercussions on civilian infrastructure when exclusively military computers or computer systems are targeted due to the interconnectedness of cyber space, on the other, there is serious concern that civilian infrastructure will be severely affected by cyber operations in armed conflicts. Thus, the principle of proportionality becomes a crucial rule for the protection of the civilian population.

The principle of proportionality is formulated in Article 51(5)(b) of Additional Protocol I, which reflects customary international law.[125] An attack is prohibited if it 'may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated'.

As said above, damage to objects means 'harm . . . impairing the value or usefulness of something . . .'.[126] Thus, it is clear that the damage to be taken into account comprises not only physical damage, but also the loss of functionality of civilian infrastructure even in the absence of physical damage. It has been argued that 'cyber attacks may change the weight given to temporary consequences' in the

123 D. E. Sanger, above note 23.
124 This follows not only from AP I, Art. 36 for states party to the Protocol, but also from the general obligation of belligerent parties not to employ indiscriminate weapons.
125 *Study on customary international humanitarian law*, above note 87, Rule 14.
126 *Concise Oxford Dictionary*.

proportionality assessment,[127] but there is no legal basis for this in IHL. As Geiss and Lahmann put it, any other reading would have the consequence that:

> whereas the destruction of a single civilian car would amount to legally relevant, albeit rather insignificant, 'collateral damage', the disconnection of thousands or millions of households, companies and public services from the internet or other communication services, or the severance of online financial transactions for a country's entire economy and the corresponding economic and societal effects as such would not count as relevant elements to be factored into the proportionality calculus.[128]

It should be recognized, however, that if and when computer network attacks do cause damage to civilian infrastructure, including by temporarily disrupting it, the principle of proportionality suffers from a number of limitations (as it also does in traditional warfare).

First, as in all applications of the principle of proportionality, there remains a measure of uncertainty about what can be considered as excessive incidental damage to civilian objects as compared to the concrete and direct military advantage. Findings that incidental damage to civilian infrastructure is excessive as compared to the military advantage appear to be few and far between.[129] This is not to say that proportionality poses no limits at all to attacks. But it remains to be seen how it will be interpreted with respect to cyber attacks.

On the one hand, it may be argued that since cyber operations are still in their infancy, little is known about their impact and commanders cannot be expected to anticipate their effects, and it is difficult to know what is 'expected' incidental civilian loss or damage in cyber warfare. On the other hand, this uncertainty is quantitative rather than qualitative; precisely because of the interwoven networks, the consequences for civilian infrastructure are obvious. In other words, incidental damage must be expected in most cases, even if its exact extent is difficult to assess.

Second, while it is by now largely undisputed that reverberating effects – that is, indirect second- or third-tier effects from an attack – must be taken into account, there remains some discussion as to how far this obligation

127 Oona Hathaway *et al.*, 'The law of cyber-attack', in *California Law Review*, Vol. 100, No. 4, 2012, p. 817.
128 R. Geiss and H. Lahmann, above note 61, p. 17.
129 See Louise Doswald-Beck, 'Some thoughts on computer network attack and the international law of armed conflict', in Michael N. Schmitt and Brian T. O'Donnell (eds), *Computer Network Attack and International Law,* International Law Studies, Vol. 76, 2002, p. 169 : '… examples … have usually been when either the possible target was something that was military in nature but in the circumstances unusable or where the object's value as a military objective could not be verified.' See also, ICTY, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia* (hereinafter *Final Report to the Prosecutor*), 13 June 2000, para. 19. In response to the bombardment of the Pancevo industrial complex and of a petroleum refinery in Novi Sad by NATO forces during the war in Kosovo in 1999, which lead to the release of some 80,000 tonnes of crude oil into the soil and of many tonnes of other toxic substances, the Committee stated that '[i]t is difficult to assess the relative values to be assigned to the military advantage gained and harm to the natural environment, and the application of the principle of proportionality is more easily stated than applied in practice'.

goes.[130] Considering the wording of Article 51(5)(b) of Additional Protocol I ('may be expected'), it is reasonable to argue that foreseeable damages, even if they are long-term, second- and third-tier damages, must be taken into account.[131] In cyberspace, because of the interconnectedness of networks, it may be more difficult to foresee the effects than with a classic kinetic weapon, but at the same time it is all the more critical to do everything feasible to assess those effects. In practical terms this leads mainly to the question of precautions to be taken in attacks. Given the interconnectedness of information networks and the systems that rely on them, what can be expected of a commander in terms of verification in order to assess what the reverberating effects of the computer network attack will be?[132]

The principle of precaution

The principle of precaution in IHL has two aspects: precautions in attack and precautions against the effects of attacks.[133]

Precautions in attack

In the conduct of military operations constant care must be taken to spare the civilian population or civilian objects.[134] Particular precautions required by IHL include doing everything feasible to verify that targets are military objectives,[135] and taking all feasible precautions in the choice of means and methods of warfare with a view to avoiding and in any event minimizing incidental civilian casualties and damages to civilian objects.[136] It also requires that parties to the conflict cancel or suspend an attack if it becomes apparent that it will cause excessive 'collateral damage'.[137]

Thus, precautions may entail such obligations as taking measures to gather all available information to verify the target and the potential incidental effects of an attack.[138] In cyber warfare, precautions may include mapping the network of

130 See, *e.g., Commentary on HPCR Manual on Air and Missile Warfare*, above note 86, Commentary on Rule 14, para. 4; Michael N. Schmitt, 'Computer network attack: the normative software', in *Yearbook of International Humanitarian Law*, The Hague, TMC Asser Press, 2001, p. 82.

131 *Tallinn Manual*, above note 27, Commentary on Rule 51, para. 6; R. Geiss and H. Lahmann, above note 61, p. 16.

132 This must be differentiated from an indiscriminate attack in which the effects cannot be controlled.

133 See AP I, Arts 57 and 58; *Study on customary international humanitarian law*, above note 87, Rules 15–24.

134 AP I, Art. 57(1); *Study on customary international humanitarian law*, above note 87, Rule 15.

135 AP I, Art. 57(2)(a)(i); *Study on customary international humanitarian law*, above note 87, Rule 16.

136 AP I, Art. 57(2)(a)(ii); *Study on customary international humanitarian law*, above note 87, Rule 17.

137 AP I, Art. 57(2)(b); *Study on customary international humanitarian law*, above note 87, Rule 19.

138 ICTY, *Final Report to the Prosecutor*, para. 29: In its Final Report, the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia described the obligation thus: 'A military commander must set up an effective intelligence gathering system to collect and evaluate information concerning potential targets. The commander must also direct his forces to use available technical means to properly identify targets during operations. Both the commander and the aircrew actually engaged in operations must have some range of discretion to determine which available resources shall be used and how they shall be used.'

the adversary,[139] which will often be part of the development of computer network attacks in any case if they are specifically designed for a particular target computer system. If the information available is incomplete – as might be the case in cyber space due to its interconnectedness – the scope of the attack might have to be limited to only those targets on which there is sufficient information.[140]

The principle of precaution might require special technical expertise. The *Tallinn Manual* states that '[g]iven the complexity of cyber operations, the high probability of affecting civilian systems, and the sometimes limited understanding of their nature and effects on the part of those charged with approving cyber operations, mission planners should, where feasible, have technical experts available to assist them in determining whether appropriate precautionary measures have been taken'.[141] If expertise, and therefore the capacity to evaluate the nature of the target or the incidental civilian loss or damage, is not available, the attacker might have to refrain from the attack.

It is likely, however, that many cyber attacks in defence will be automatic, pre-programmed cyber operations against intrusions from the outside.[142] Such 'hack-backs' are automatic and simply target the computers from which the intrusion originates; as they are tackling a technical problem, they are not concerned with the civilian or military nature of the computers. In such contexts, and given that such cyber attacks will come from thousands or even millions of computers, states will have to carefully evaluate the lawfulness of such automatic hack-backs in light of the principle of precaution.

From another angle, the principle of precaution could, in some instances, entail an obligation to resort to cyber technology when it is available. Indeed, cyber operations might also cause less incidental damage to civilians or civilian infrastructure than kinetic operations. For instance, it might be less damaging to disrupt certain services used for military and civilian purposes than to destroy infrastructure completely. However, the extent of an obligation to resort to more sophisticated technology – in this case cyber technology – is not entirely settled. Indeed, there is as yet no international consensus that belligerent parties must at all times employ the most precise or the most technologically advanced weapon (the discussion on this issue mainly takes place with respect to precision-guided munitions).[143] Nonetheless, the principle of precaution contains an obligation not only to abide by the principles of distinction and proportionality, but also to do everything feasible to 'avoid and in any event minimize' incidental civilian loss or damage. In such cases, the principle of precaution arguably implies that

139 E. T. Jensen, above note 90, p. 1185.
140 *Tallinn Manual*, above note 27, Rule 53, para. 6.
141 *Ibid.*, Rule 52, para. 6.
142 According to AP I, Art. 49, such defensive operations are also attacks' that have to abide by the principles of distinction, proportionality, and precaution.
143 See Jean-François Quéguiner, 'Precautions under the law governing the conduct of hostilities', in *International Review of the Red Cross*, Vol. 88, No. 864, December 2006, p. 801; *Commentary on HPCR Manual on Air and Missile Warfare*, above note 86, Commentary on Rule 8, para. 2.

commanders should choose the less harmful means available at the time of the attack to achieve their military aim.[144]

Precautions against the effects of attacks

The principle of precautions against the effects of attacks requires that the parties to conflicts, among others, 'to the maximum extent feasible . . . endeavour to remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives' and 'take the other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers arising from military operations'.[145] This means that states have an obligation to either keep military objects apart from civilians and civilian objects, or (and particularly if this is not feasible) to take other measures to protect civilians and civilian infrastructure from the dangers resulting from military operations.

As the Tallinn Manual states, this may include 'segregating military from civilian cyber infrastructure; segregating computer systems on which critical civilian infrastructure depends from the Internet; backing up important civilian data elsewhere; making advance arrangements to ensure the timely repair of important computer systems against foreseeable kinds of cyber attack; digitally recording important cultural or spiritual objects to facilitate reconstruction in the event of their destruction during armed conflict; and using antivirus measures to protect civilian systems that might suffer damage or destruction during an attack on military cyber infrastructure'.[146]

It is indeed frequently advocated that military and civilian networks should be segregated.[147] As the legal assessment of the US Department of Defense recommends, 'where there is a choice, military systems should be kept separate from infrastructures used for essential civilian purposes'.[148] However, this is hardly realistic. In the early days of the Internet, construction probably proceeded without consideration for these matters. There exist, of course, closed military networks, and certain highly sensitive civilian infrastructure is also segregated from outside networks. But considering the inherent weakness of the rule on segregating civilian from military objects (Article 58(a) of Additional Protocol I), which only obliges states to endeavour to separate military and civilian objects and only to the maximum extent feasible, it is highly unlikely that it will be interpreted in state practice as entailing an obligation to segregate civilian and military networks. While it might theoretically be feasible to do this, it would be so impractical and costly as to

144 K. Dörmann, above note 42; Michael N. Schmitt, 'The principle of discrimination in 21st century warfare', in *Yale Human Rights and Development Law Journal*, Vol. 2, 1999, p. 170; *Commentary on HPCR Manual on Air and Missile Warfare*, above note 86, Commentary on Rule 32(b), para. 3, on weapons with greater precision or lesser explosive force.

145 AP I, Art. 58; *Study on customary international humanitarian law*, above note 89, Rules 22 and 24.

146 *Tallinn Manual*, above note 27, Commentary on Rule 59, para. 3.

147 E. T. Jensen, above note 97, pp. 1533–1569; Adam Segal, 'Cyber space governance: the next step', Council on Foreign Relations, *Policy Innovation Memorandum No. 2*, 14 November 2011, p. 3, available at: http://www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397.

148 Department of Defense Office of General Counsel, above note 112, p. 7.

be seen as unfeasible in the sense of Article 58 of Additional Protocol I. Governments would have to create their own computer hardware and software for military use and establish their own military lines of communication, including cables, routers, and satellites, throughout the world.[149]

In addition, the separation of military from civilian cyber infrastructure rests on the assumption that they are distinct and should be kept distinct. Strictly speaking, Article 58 does not prohibit dual use: it rests on the assumption that there is a differentiation between civilian and military objects, even if some civilian objects are used as military objectives. Already in the physical world, large parts of critical infrastructure are dual use, for example, electrical grids, but also, in many instances, oil pipelines, power plants, and road networks. In cyber space the principle becomes relatively meaningless where the problem is not the co-location of civilian and military infrastructures but the fact that it is one and the same.[150]

The question, then, is whether Article 58(c) of Additional Protocol I would require that at least some civilian infrastructure (for instance, nuclear power stations, chemical factories, hospitals) is protected against damage in the case of a cyber attack, requiring that states take action to maintain its functionality. For instance, Eric Talbot Jensen recommends that, in order to comply with its obligation under Article 58, the US take a number of measures such as mapping the civilian systems, networks, and industries that will become military objectives, ensure that the private sector is sufficiently protected, establish or maintain hack-back solutions, or create a strategic reserve of Internet capability.[151] The tendency of numerous countries to protect their critical infrastructure certainly goes in this direction – though it is unlikely that governments conceive of this protection in terms of passive precautions within the meaning of Article 58(c).

Conclusion

As noted in the introduction, cyber operations will entail new means and methods of combat, the effects of which are still untested or poorly understood. It appears, however, that military use of information technology poses serious challenges to the application of IHL, in particular with respect to the very premise that civilian and military objects can and must be distinguished in armed conflict. In order to obtain clear statements about how states intend to respect the principles of distinction, proportionality, and precaution, this should be discussed more openly and candidly than has been the case until now.

In light of the dangers that cyber warfare poses to civilian infrastructure a number of solutions are being proposed *de lege lata* and *de lege ferenda*. One proposal is for states to make declaratory statements about digital safe havens, that is, civilian targets that they will consider off-limits in the conduct of cyber

149 E. T. Jensen, above note 97, pp. 1551–1552.
150 See also R. Geiss and H. Lahmann, above note 61, p. 14.
151 E. T. Jensen, above note 97, pp. 1563 ff.

operations.[152] If agreed among the parties, this would be akin to the demilitarized zones foreseen in Article 60 of Additional Protocol I. It would require the process of dialogue and confidence-building measures currently advocated, which go beyond the subject of this article. Adam Segal stipulates that 'there is likely to be relatively easy consensus around some areas – hospitals and medical data – and much less agreement around others such as financial systems, power grids, and Internet infrastructure'.[153] While this is an interesting path to explore – and might ultimately be explored as part of an international dialogue on confidence-building measures – it is probably not being overly pessimistic to be sceptical about the short-term feasibility of this avenue. Given the concealed nature of much of what appears to be the current manipulation and infiltration of cyber space, it is not clear how much trust will be put in agreements or statements on cyber areas that would be off-limits for military use.

Another proposal made by Geiss and Lahmann is to expand the list of 'works and installations containing dangerous forces' in Article 56 of Additional Protocol I by analogy.[154] This could apply to specific cyber infrastructure components, such as major Internet exchange nodes or central servers on which millions of important civilian functions rely. Just like dams, dykes, and nuclear electrical generating stations, they could not be made the object of attack even if they constituted military objectives because the dangers for the civilian population would always be considered to outweigh the military advantage of attacking them. However, Geiss and Lahmann also acknowledge that it is unlikely that such a proposal would find favour among states. In particular, although the reverberating effects of neutralizing or destroying cyber infrastructure could be momentous, it would be difficult to argue that they would be comparable to the release of emissions such as radioactive material or the waters of a dam. If, however, they had such comparable disastrous effects, the underlying rationale of Article 56 of Additional Protocol I could equally provide a persuasive argument to protect cyber infrastructure.

Going further, the challenges posed by the cyber realm have also raised the question whether (some) means and methods of cyber warfare should be banned altogether or regulated by international treaty. As mentioned in the introduction, some states have advocated for a new treaty in this respect, although the contours of what should and should not be allowed are not always entirely clear. A parallel debate is also being held among cyber security experts and academics. Some have proposed new treaties on cyber warfare,[155] while others argue that there should be a type of disarmament treaty with a ban on all or at least some cyber weapons.[156]

152 A. Segal, above note 147.
153 *Ibid.*
154 R. Geiss and H. Lahmann, above note 61, p. 11.
155 Mark R. Shulman, 'Discrimination in the law of information warfare', in *Columbia Journal of Transnational Law*, Vol. 37, 1999, p. 964; Davis Brown, 'A proposal for an international convention to regulate the use of information systems in armed conflict', in *Harvard International Law Journal*, Vol. 47, No. 1, Winter 2006, p. 179; Duncan B. Hollis, 'Why states need an international law for information operations', in *Lewis and Clark Law Review*, Vol. 11, 2007, p. 1023.
156 Mary Ellen O'Connell, 'Cyber mania', in *Cyber Security and International Law*, Meeting Summary, Chatham House, 29 May 2012, available at: http://www.chathamhouse.org/sites/default/files/public/

Still others counter that a treaty would not be enforceable because of the difficulties of attribution, that it would be technically impossible to distinguish between instruments of cyber warfare and cyber espionage, that the banned weapons could be less damaging than traditional weapons, and that verification would be impossible.[157]

Some commentators propose other solutions, such as 'informal multilateralism',[158] or an international cyber security organisation, along the lines of the International Atomic Energy Agency, as an independent platform for international cooperation, with the aim of developing treaties to control cyber weapons.[159]

It is difficult to know, at this point, where these discussions will lead, and especially whether states are willing to discuss the real dangers of cyber warfare openly and to take measures to prevent the worst-case scenarios. In the meantime, if parties to conflicts choose cyber weapons during armed conflicts they must be aware of the existing legal framework as a minimum set of rules to respect, despite their limitations. They must instruct and train their forces accordingly. It is important to promote the discussion of these issues, to raise awareness of the need to assess the humanitarian impact of developing technologies, and to ensure that they are not prematurely employed under conditions in which respect for the law cannot be guaranteed.

In conclusion, there is no question that IHL applies to cyber warfare. However, whether it will provide sufficient protection to the civilian population, in particular by shielding civilian infrastructure from harm, will depend on how IHL – whose drafters did not envisage such operations – is interpreted with respect to them. Only if interpreted in good faith and with the utmost care will it be possible to protect civilian infrastructure from being directly targeted or from suffering damage that could potentially be disastrous for the civilian population. Even then, considering the potential weaknesses of the principles of distinction, proportionality, and precaution – and in the absence of more profound knowledge of offensive capabilities and effects – it cannot be excluded that more stringent rules might be necessary.

Research/International%20Law/290512summary.pdf; Misha Glenny, 'We will rue Stuxnet's cavalier deployment', in *The Financial Times*, 6 June 2012, citing Russian antivirus expert Eugen Kaspersky; Scott Kemp, 'Cyberweapons: bold steps in a digital darkness?', in *Bulletin of the Atomic Scientists*, 7 June 2012, available at: http://thebulletin.org/web-edition/op-eds/cyberweapons-bold-steps-digital-darkness; Bruce Schneier, 'An international cyberwar treaty is the only way to stem the threat', in *US News*, 8 June 2012, available at: http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/an-international-cyberwar-treaty-is-the-only-way-to-stem-the-threat; Duncan Holis, 'An e-SOS for cyberspace', in *Harvard International Law Journal,* Vol. 52, No. 2, Summer 2011, who argues for a system of e-sos.

157 Herb Lin and Thomas Rid, 'Think again: cyberwar', in *Foreign Policy,* March/April 2012, p. 7, available at: http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?print=yes&hidecomments=yes&page=full; Jack Goldsmith, 'Cybersecurity treaties: a skeptical view', in Peter Berkowitz (ed.), *Future Challenges in National Security and Law* (forthcoming), available at: http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf.

158 A. Segal, above note 108.

159 Eugene Kaspersky, 'Der Cyber-Krieg kann jeden treffen', in *Süddeutsche*, 13 September 2012, available at: http://www.sueddeutsche.de/digital/sicherheit-im-internet-der-cyber-krieg-kann-jeden-treffen-1.1466845.

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

Some legal challenges posed by remote attack

William Boothby

Dr William Boothby retired in July 2011 as Deputy Director of Legal Services (Royal Air Force) in the rank of Air Commodore. His doctoral thesis on *Weapons and the Law of Armed Conflict* was published by Oxford University Press (OUP) in 2009 and his second book, *The Law of Targeting*, was published by OUP in August 2012.

Abstract

Attacking from a distance is nothing new, but with the advent of certain new technologies, attacks can be undertaken in which the attacker remains very remote from the scene where force will be employed. This article analyses the legal issues raised by attacks employing, respectively, remotely piloted vehicles, autonomous attack technologies, and cyber capabilities. It considers targeting law principles and rules, including distinction, discrimination, proportionality, and the precautions rules, observes that they all apply to remote attack and proceeds to explore the challenges that arise from implementing the legal requirements. Due note is taken of states' legal obligation to review new weapons, methods and means of warfare, an obligation that reinforces the view that existing law will provide the prism through which these new attack technologies must be evaluated by states. The article then discusses how notions of liability apply in relation to remote attack, and considers whether it is depersonalization rather than remoteness in attack that is the critical legal issue.

Keywords: remote attack, remotely piloted vehicles, unmanned aerial vehicles (UAVs), cyber attack, autonomous attack, legal review of new weapons, means or method of warfare, liability.

In a report dated 29 November 2011, *The Guardian* newspaper asked '[w]hy did NATO forces kill two dozen Pakistani soldiers at a border post in the Mohmand

doi:10.1017/S1816383112000719

region, some 300 yards across the frontier from Afghanistan early on Saturday morning?'[1] Having reflected upon differing explanations for the event, the report asserted '[t]here is a very simple explanation of what happened, the US military makes deadly mistakes all the time, and for all its technological wizardry and tremendous firepower, it has very little intelligence on the ground'. Reportedly, in 2010 'a U.S. military investigation . . . harshly criticized a Nevada-based Air Force drone crew and American ground commanders in Afghanistan for misidentifying civilians as insurgents during a U.S. Army Special Forces operation in Oruzgan province in February, resulting in the deaths of as many as 23 civilians'.[2]

From one kind of 'military operations from a distance', or remote attack as we shall call the phenomenon, let us move to another, namely cyber operations. Military use of cyber operations[3] occurred on 27 and 28 April 2007 when an apparently coordinated sequence of denial-of-service operations affected websites in Estonia during a dispute between that country and Russia. Ping requests were followed by malformed Web queries to governmental and media websites. From 30 April until 18 May 2007, distributed operations aimed at producing a denial of service from targeted websites (distributed denial of service or DDoS) followed. Careful timing of cyber operations maximized their effectiveness, and the affected sites became temporarily inaccessible. It appeared that botnets were being employed and a precise impact was the evident result.[4] Some Estonian websites were defaced by so-called patriotic hackers, but it was never formally determined which state, if any, was responsible.[5] Then, in 2008, cyber operations were undertaken against Georgia during its armed conflict with Russia.

The 2010 Stuxnet operation against Iran was, perhaps, one of the more militarily significant cyber operations. Stuxnet is an integrated set of components that were used to undertake computer network attacks. Using, in part, a worm as its delivery mechanism, Stuxnet inserts itself onto disconnected networks, for example through the use of thumb drives or CD-ROMs. It searches for a specified manufacturer's model of computer control facility – in the case of the Iranian attack

1 P. Chatterjee, 'Should we allow NATO free rein to attack and kill people?', in *The Guardian,* 29 November 2011, available at: http://www.guardian.co.uk/commentisfree/2011/nov/29/nato-free-range-to-kill (this and all subsequent links last visited April 2012).

2 For reference to the earlier cited incident, see David Zucchino, 'US Report faults Air Force drone crew, ground commanders in Afghan civilian deaths', in *Los Angeles Times*, 29 May 2010, available at: http://articles.latimes.com/2010/may/29/world/la-fg-afghan-drone-20100531.

3 Cyber operations are taken for the purposes of this article to consist of the use of a computer to interact with another computer for purposes linked to a military operation. Cyber attack is therefore, for similar purposes, the use of a computer to target another computer and thus to cause violent effects, consisting of damage or destruction to property or death or injury to persons. See Michael N. Schmitt, 'Cyber operations and the *jus in bello*: key issues', in *International Law Studies*, Vol. 87, 2011, pp. 93–94.

4 Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations*, CCD COE Publications, Talllinn, 2010, pp. 18–25. Note also that a DDoS operation on 26–28 April 2008, which targeted the website of Radio Free Europe/Radio Liberty's Belarus service, is reported and discussed at E. Tikk, *ibid*., pp. 39–48, as is a cyber operation that targeted Lithuania on 17 June 2008, E. Tikk, *ibid*., pp. 51-64.

5 William A. Owens, Kenneth W. Dam and Herbert S. Lin, *Technology, Policy, Law and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities*, National Research Council of the National Academies, The National Academies Press, Washington D.C., 2009, pp. 173–176.

a control system manufactured by Siemens – finds and places itself on a relevant node and undertakes pre-planned activity. During the July 2010 operation, malware reportedly attacked centrifuges evidently associated with the Iranian nuclear programme and, it appears, caused damage.[6] While the defacement of websites as exemplified in the Estonian operations would not seem to amount to an attack in the *in bello* sense,[7] it is likely that the Stuxnet attack would be regarded at law as such an attack because of the damage reportedly caused to the centrifuges.

The use, during armed conflicts, of these cyber techniques to prosecute attacks, that is to cause death, injury, damage or destruction, or the employment of remotely piloted[8] or, in the future, autonomous unmanned platforms to undertake attacks constitutes what, for the purposes of this article, we shall describe as 'remote attack'. Such attacks are remote in the sense that the operator of the remotely piloted vehicle or the initiator of the autonomous mission or of the cyber attack is liable to be located at a considerable distance from the scene of the injury or destruction wrought by the attack. The purpose of the present article is to consider whether the remote conduct of attacks using such techniques during armed conflicts raises legal concerns. The author's starting point is that cyber attacks during armed conflict, namely military operations in which cyber means are employed to inflict death, injury, damage or destruction on an adverse party to the conflict, are regulated by the law of armed conflict and thus, for states party to the Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (API),[9] are subject to the rules in Articles 48 to 67 of that treaty.[10] For states that are not party to API, the customary principles and rules – most notably the customary principle of distinction and the customary rules of discrimination, of proportionality, and of precautions in attack – will

6 It is understood that these reports of damage have not been confirmed by Iran. See, however, Jonathan Fildes, 'Stuxnet worm "targeted high value Iranian assets"', in *BBC News*, 23 September 2010, available at: http://www.bbc.co.uk/news/technology-11388018; and William J. Broad, John Markoff and David E. Sanger, 'Israeli test on worm called crucial in Iran nuclear delay', in *New York Times*, 15 January 2011, available at: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all.

7 See Article 49(1) of API, which defines attacks in terms of the use of violence, whether in offence or defence.

8 As to the controversies raised by the use of unmanned platforms to conduct attacks during current operations, see for example Karen DeYoung, 'U.S. officials cite gains against Al-Qaeda in Pakistan', in *Washington Post*, 1 June 2009, available at: http://www.washingtonpost.com/wp-dyn/content/article/2009/05/31/AR2009053102172.html; the associated analysis by Kenneth Anderson in 'The continuing predator drone campaign in Pakistan', in *Opinio Juris Blog*, 1 June 2009, available at: http://opiniojuris.org/2009/06/01/the-continuing-predator-drone-campaign-in-pakistan/; and Karen DeYoung, 'CIA idles drone flights from base in Pakistan', in *Washington Post*, 1 July 2011, available at: http://www.washingtonpost.com/world/national-security/cia-idles-drone-flights-from-base-in-pakistan/2011/07/01/AGpOiKuH_story.html. As to US appreciation of the strategic importance of attacks on Al Qaeda often carried out using unmanned platforms, see Eric Schmitt and Mark Mazzetti, 'Obama adviser outlines plans to defeat Al Qaeda', *New York Times*, 29 June 2011, available at: http://www.nytimes.com/2011/06/30/world/30terror.html.

9 Adopted in Geneva, 8 June 1977.

10 For a discussion of this issue, see Michael N. Schmitt, 'Cyber operations and the *jus in bello*: key issues', in *US Naval War College Blue Book*, 'International Law and the Changing Character of War', Vol. 87, 2011, p. 89.

apply.[11] Similarly, it seems to be generally accepted that the same body of law regulates attacks using unmanned platforms, that is aircraft, ground vehicles, ships or other marine craft that do not carry crew personnel and that are either controlled by an operator who is located remotely from the relevant platform or that employ autonomous guidance and attack technology.[12] We will discuss these issues primarily by reference to the air domain and will call such operator-controlled vehicles 'remotely piloted vehicles', while references to autonomy will be applied to platforms that make attack decisions without the supervision of a human being. In relation to both such methods of attack, the question to be discussed is therefore whether the absence of the person who is undertaking the attack from the location of its operative effect raises legal concerns.

We shall start by considering attacks using remotely piloted platforms. We will then briefly outline the issues in relation to precautions in attack posed by the use of autonomous attack technologies. In the third section of the article we will summarize how the targeting rules in API can be applied to cyber attacks. Then, in the fourth section, we will analyse where the remoteness challenge sits. In the fifth section we will discuss where liability may rest for these differing classes of attack. In the final substantive section we will ask whether these new technologies represent a qualitative change in the conduct of warfare or a further development in a well-established evolutionary process, essentially posing the question whether what we are discussing is really anything substantively new. We will then seek to draw conclusions.

Remotely piloted vehicles and the law

The remoteness of the controller from the attack does not, per se, exclude the application of targeting law to such activities. The legal principle of

11 In practice, many of the rules in API, Articles 48 to 67, are customary in nature and thus bind all states; see Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian* Law, *Vol. 1: Rules*, Cambridge University Press, 2005 (hereafter 'ICRC Study'). While in the view of the present author the rules in Articles 35(3), 55 and 56 of API have not achieved customary status, note for example the principle of distinction as reflected in the ICRC Study, rule 1 at page 3: 'The parties to the conflict must at all times distinguish between civilians and combatants. Attacks may only be directed against combatants. Attacks must not be directed against civilians'. Note also the International Court of Justice (ICJ) finding that the principle of distinction is 'an intransgressible principl[e] of international customary law', International Court of Justice, *Advisory Opinion on the Threat or Use of Nuclear Weapons*, ICJ Reports, 8 July 1996, p. 257, para. 79. The ICRC Study reflects the principle of discrimination in its rule 11 at page 37, rule 12 at page 40, rule 13 at page 43, and rule 14 at page 46. These rules respectively prohibit indiscriminate attacks, spell out what such attacks comprise, and then reflect Article 51(5)(a) and (b) of API which, it will be recalled, are described in the treaty as examples of indiscriminate attacks. Customary law also recognizes a rule that requires attackers to take certain precautions in attacks. These customary precautionary rules are reflected in the ICRC Study at rules 18 to 21 on pages 58 to 65. For a discussion of the customary law of targeting, see William H. Boothby, *The Law of Targeting*, Oxford University Press, Oxford, 2012, Chapter 5.

12 See, for example, the discussion in 'Targeting operations with drone technology: humanitarian law implications', in *Background Note for the American Society of International Law Annual Meeting*, Human Rights Institute, Columbia Law School, 25 March 2011.

distinction,[13] the prohibition of indiscriminate attacks,[14] the precautions rules, and the more detailed provisions requiring the protection of specific persons and objects[15] will all apply to such operations. The controller of a Predator or Reaper Unmanned Aerial Vehicle (UAV), although located some thousands of miles from the scene of the attack, bases his attack decisions on the information derived from sensors and other sources and is as constrained by the targeting rules, including the rules as to precautions in attack, as any other military operator in the battle space, including a pilot of a manned aircraft.

Accordingly, the UAV operator must take constant care to spare civilians and civilian objects when undertaking military operations in general;[16] he must do everything practicable or practically possible[17] to 'verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives . . . and that it is not prohibited . . . to attack them'; he must take all practicable or practically possible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects;[18] he must 'refrain from deciding to launch any attack which may be expected' to cause disproportionate incidental civilian injury and/or damage;[19] he must cancel or suspend the attack if it becomes clear that its objective is not a military objective, that its objective is subject to special protection or that the attack may be expected to cause disproportionate incidental civilian injury or damage;[20] he must ensure that an effective advance warning is given if civilians may be affected by the attack unless circumstances do not permit;[21] and he must ensure that 'when a choice is possible between several military objectives for obtaining a similar military advantage, the objective that is selected is the objective 'the attack on which may be

13 Article 48 of API requires that 'in order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives'. The notion of 'military objective' is defined, so far as objects are concerned, in Article 52(2) of API.

14 By virtue of Article 51(4) of API, attacks are indiscriminate and therefore prohibited if they are not directed at a specific military objective, if they employ a method or means of combat that cannot be directed at a specific military objective, or the effects of which cannot be limited as required by international law, and in any such case are of a nature to strike the military objective and civilians or civilian objects without distinction. An attack that may be expected to cause excessive incidental injury to civilians and/or damage to civilian objects is stated at Article 51(5) to be an example of an indiscriminate attack.

15 For example, the prohibitions on making the civilian population, individual civilians, or civilian objects the object of attack in Articles 51(2) and 52(1) of API.

16 Article 57(1) of API.

17 The language used in Article 57(2)(a)(i) is 'everything feasible', which the UK interprets as everything 'practicable or practically possible taking into account all circumstances ruling at the time including humanitarian and military considerations'; UK statement (b) made on ratification of API on 28 January 1998. Consider also Eritrea/Ethiopia Claims Commission, *Partial Award, Central Front, Ethiopia's Claim 2*, 28 April 2004, para. 110, available at: http://www.pca-cpa.org/showpage.asp?pag_id=1151.

18 Article 57(2)(a)(ii) of API.

19 Article 57(2)(a)(iii) of API.

20 Article 57(2)(b) of API.

21 Article 57(2)(c) of API.

expected to cause the least danger to civilian lives and to civilian objects'.[22] These precautionary rules bind parties to API as a matter of treaty law and, as we noted above, are largely customary and thus bind all states. It follows from this analysis that the precautionary duties of a controller of an armed UAV are just as exacting as those imposed on the pilot of a manned aircraft. The law does not reduce these duties because of the absence of a person from the cockpit.[23]

Autonomous attack and the law

The word 'autonomy' is taken for the purposes of the present discussion to refer to autonomous attack decision-making undertaken by, for example, algorithm-based technology on board an unmanned platform such as an aerial vehicle.[24] The technology may, for example, be programmed to detect points of recognition of particular military objects, such as a tank, artillery piece or armoured personnel carrier. If the technology adequately distinguishes between such military objects and civilian objects, it would seem that the requirement in Article 57(2)(a)(i) of API[25] may be complied with, provided it can properly be said that 'everything feasible' is being done to accomplish the required distinction. In the light of the United Kingdom (UK) interpretative statement cited above,[26] military considerations may be taken into account in order to determine that which is practically possible and thus required as a feasible precaution. An argument that the absence of a human being from the autonomous aspect of the decision-making process renders the performance of these precautionary duties impractical and that they are therefore to be regarded as militarily non-feasible would, in the author's view, be unsatisfactory, not least because alternative methods of undertaking such attacks would permit of the taking of such precautions. The better view must therefore be that the full set of precautionary measures set out in Article 57 of API and summarized in the previous section of this article must be complied with in relation to autonomous attacks.

While compliance with Article 57(2)(a)(i) of API may be achievable as discussed in the previous paragraph,[27] things get somewhat more difficult when we

22 Article 57(3) of API.

23 The interesting question is whether the absence of a person from the cockpit renders compliance with the rules easier or more difficult. Providing an answer would involve considering whether direct, as opposed to sensor-based observation of the intended target by the person deciding on the particular attack would have been feasible in the relevant circumstances had a manned platform been used; whether such direct observation in the prevailing circumstances would have made any difference to the quality of attack decision-making; whether enemy action may have diverted the pilot's attention from the targeting task; whether other distractions would have been present; and relevant and numerous other issues.

24 The word 'autonomy' is sometimes used to refer to aspects of the navigational system of the platform. In the present article, it specifically refers to the method of attack, and particularly to the method whereby the weapon's target is selected.

25 This requirement is customary in nature; see rule 18 of the ICRC Study and the discussion at W. Boothby, above note 11, p. 73.

26 See above note 17.

27 See Bill Boothby, 'The law relating to unmanned aerial vehicles, unmanned combat aerial vehicles and intelligence gathering from the air', in *Humanitäres Völkerrecht – Informationsschriften*, Vol. 24, issue 2, 2011, p. 81.

consider the evaluative rules of precaution. These further precautionary duties, listed in the previous section and which do not require repetition here, generate the challenging question of whether technology is capable of mechanizing essentially evaluative judgements. These include the assessment of whether the chosen means and method for undertaking the planned attack will in fact minimize injury to civilians and damage to civilian objects and whether the injury to civilians and the damage to civilian objects that may be expected to result from the attack of a given class of military objective on a specified occasion will be excessive in relation to the anticipated military advantage. The statement by the UK and other states on ratification of API, to the effect that military advantage is intended to refer to that accruing from the attack considered as a whole,[28] suggests that the proportionality assessment should be applied to something more that an individual engagement of a single object.[29]

Nevertheless, a means or method of warfare[30] is likely to prove legally unacceptable if it precludes the taking of these legally required evaluative precautions. Autonomous attack methods will not, however, necessarily preclude the taking of these precautions. Thus, planners and operational decision-makers contemplating the mounting of an autonomous mission are likely to be in a position to review relevant pattern-of-life data relating to the planned area of search. They will review that data in order to assess, before the commencement of the autonomous mission, the civilian death, injury, and damage that may be expected as a result of an attack of the planned class of military objective in that area during the planned period of search using the weapons loaded onto the platform. The military advantage to be anticipated from the successful attack of an object that the algorithm technology is programmed to recognize will be known at the planning stage, so, depending on the pattern of life in the relevant area, it may be possible to comply with the evaluative precautionary rules at the mission planning stage thus rendering the use of autonomous attack technology potentially lawful. This is most likely to be the case if the planned area of search is remote from civilians and civilian objects; areas of desert, remote steppe lands, and remote maritime areas would seem to be examples. It may also be the case if, for whatever reason, pattern-of-life data clearly show that civilians will remain absent from a less remote area at the time of the planned search.

If, by contrast, judgements as to the minimization of civilian death, injury, and damage and as to the proportionality of attacks cannot be made at the sortie planning stage, for example because of the congested urban nature of the area of

28 UK statement (i) made on ratification of API on 28 January 1998.

29 The statement was made by reference to Articles 51 and 57. Viewing individual hostile acts in isolation 'would ignore the problems resulting from modern strategies of warfare, which are invariably based on an integrated series of separate actions forming one ultimate compound operation . . . The aggregate military operation of the belligerent may not be divided up into too many individual actions, otherwise the operative purpose for which the overall operation was designed slips out of sight'. Stefan Oeter, 'Methods and means of combat', in D. Fleck (ed.), *The Handbook of International Humanitarian Law*, 2nd edn, 2009, p. 186.

30 The particular platform will form part of the weapon system associated with the relevant missile, etc. It will be a part of that means of warfare.

search or because for whatever reason civilian death, injury, and damage cannot be predicted with acceptable assurance in advance of the mission, it follows that the evaluative precautions cannot be undertaken with the consequence that a decision to undertake an autonomous mission in such circumstances would breach Article 57.

The focus in this discussion is on autonomous attacks targeting inherently military objects with characteristics that facilitate mechanical recognition. So far as is known, technology is not currently available to support the autonomous distinguishing of military personnel from civilians. Only when autonomous attack technology can make those distinctions to an acceptable degree of reliability, and only when, having so distinguished, the technology enables the evaluative decisions referred to above to be made in the context of attacks that target persons will there be any basis for a discussion of autonomous attack of individuals. The author is not aware of any such system yet having been fielded, and therefore concludes that autonomous attack of personnel can, for the time being at least, be excluded on the ground that the rules as to precautions in attack cannot be complied with.[31]

Cyber attacks and the law

The computer age has brought into existence another environment in which hostilities can be conducted.[32] The dependence of modern societies and of their armed forces on computer systems renders such systems prime objects of attack, or a choice medium through which to target some linked object or person.[33] Events in Estonia in 2007,[34] in Georgia in 2008[35] and in Iran in

31 See, however, Ronald C. Arkin, *Governing Lethal Behavior in Autonomous Robots*, CRC Press Taylor & Francis Group, Boca Raton, F.A., 2009, for a discussion of technical approaches to robotic decision-making designed to overcome the issues discussed in the present section. For a statement of the technological requirements before autonomous attack is likely to become legally acceptable, see Tony Gillespie and Robin West, 'Requirements for autonomous unmanned air systems set by legal issues', in *The International C2 Journal*, Vol. 4, No. 2, 2010, pp. 1–32, available at: http://www.dodccrp.org/files/IC2J_v4n2_02_Gillespie.pdf. For a suggested ethical duty to use UAVs, see Bradley J. Strawser, 'Moral predators: the duty to employ uninhabited aerial vehicles', in *Journal of Military Ethics*, Vol. 9, No. 4, 2010, pp. 342–344. Ronald C. Arkin, 'The case for ethical autonomy in unmanned systems', in *Journal of Military Ethics*, Vol. 9, No. 4, 2010, pp. 332, analyses why humans breach the legal and moral prohibition of attacking civilians and argues that robotic attack techniques will tend to obviate such unacceptable behaviour.

32 The word 'environment' is used because views differ as to whether cyberspace can properly be described as a 'domain'; see Michael V. Hayden, 'The future of things "cyber"', in *Strategic Studies Quarterly*, Vol. 5, No. 1, Spring 2011, pp. 3–4; and John A. Shaud, 'An Air Force strategic vision for 2020–2030', in *Strategic Studies Quarterly*, Vol. 5, No. 1, Spring 2011, pp. 8–17.

33 Note, for example, the May 2009 cyber operation that shut down the US FBI computer network; Bill Gertz, 'Inside the ring', in *The Washington Times*, 18 June 2009, available at: http://www.washingtontimes.com/news/2009/jun/18/inside-the-ring-95264632/?page=all; for an indication of the scale and extent of cyber espionage, see Sean Rayment, 'How safe are Britain's cyber borders?', in *The Sunday Telegraph*, 26 June 2011, available at: http://www.telegraph.co.uk/news/uknews/defence/8598952/How-safe-are-Britains-cyber-borders.html.

34 See E. Tikk, *et al.*, above note 4, pp. 18–25; and W. A. Owens, *et al.*, above note 5, pp. 173–176.

35 J. Markoff, 'Georgia takes a beating in the cyberwar with Russia', in *New York Times*, Bits Blog, 11 August 2008, available at: http://bits.blogs.nytimes.com/2008/08/11/georgia-takes-a-beating-in-the-cyberwar-

2010[36] indicate that the offensive use of cyber operations will be an increasingly important aspect of warfare in coming decades. Cyber operations can be taken to be military operations in which one computer is used either to target another or to use that other computer as the conduit through which injury or damage is caused to an opposing party to the conflict. The use of any instrument, including a computer, to cause death, injury, damage or destruction to another party to an armed conflict will cause that instrument, or computer, to become a weapon or means of warfare.[37] The damage or injury may be caused to the users of the targeted computer system or the targeted system itself may be damaged; in either case causing the cyber operation to be regarded as a cyber attack. The critical issue for the purposes of the present article is, however, that the operation may be initiated a considerable distance in both space and time from the place and time, where and when, the damaging consequences are intended to occur. This notion of remoteness of the operator from the consequences of his or her activity is compounded by the difficulty that is likely to be encountered in determining, and then being able to demonstrate, first, who undertook the cyber operation in question, second, on behalf of which state or organization, if any, the operation was undertaken, and, third, its purpose.

A relevant legal issue arises from the difficulty that the planner and decision-maker are likely to have in evaluating in advance the expected results of a planned cyber attack. In order to make any sensible assessment of the legitimacy of the planned attack they will need to know enough about the cyber linkages between the sending computer and the targeted computer to be sufficiently assured that the attack will in fact engage the intended target. Secondly, they will also need to know enough about the characteristics of the particular cyber capability that is being used to undertake the attack to be assured that it will engage the target in the intended way. Thirdly, they will need to know enough about the targeted computer system, its dependencies, and associated networks to be able to assess the proportionality of the planned attack. Finally, if the cyber capability to be used in the attack is liable to affect other networks as it travels to the targeted system, the expected effects on those other networks will need to be assessed as, to the extent that those networks do not themselves consist of military objectives, damage to them, and consequential damage or injury to their users will have to be factored into the proportionality assessment that is made in advance of the decision to mount the cyber attack.

Mapping the targeted system, its dependencies, and the intervening linkages in this way is likely to be a challenging task. Undertaking that mapping in a covert way is likely to be even more difficult. To maintain that operational security by failing to undertake any assessment of the proportionality of the planned attack

with-russia/; European Union Independent International Fact Finding Mission on the Conflict in Georgia, Report (2009); and see also E. Tikk, *et al.*, above note 4, pp. 67–79.

36 J. Fildes, 'Stuxnet worm attacked high value Iranian assets', in *BBC News*, 23 September 2010, available at: http://www.bbc.co.uk/news/technology-11388018; and W. J. Broad, *et al.*, above note 6.

37 For the meaning of weapon see Justin McClelland, 'The review of weapons in accordance with Article 36 of Additional Protocol 1', in *International Review of the Red Cross*, Vol. 85, No. 850, June 2003, p. 397. For the meaning of 'means of warfare', see William H. Boothby, *Weapons and the Law of Armed Conflict*, Oxford University Press, Oxford, 2009, p. 4.

is likely to breach Article 57 for the same reasons as were noted in the previous section.

Where the remoteness challenge sits

What emerges from the analysis, however, is that the distance in time and space does not of itself render the attack unlawful. At the root of the problem is the effect that this remoteness has on the ability of planners and decision-makers to undertake required precautions and to obtain information to support a sensible evaluation of the lawfulness of the planned attack. To put the matter simply, it is only when the technological advances that enable remote attack, be it cyber, autonomous or remotely piloted, are matched by the technological capability to inform the standard precautions the law requires in relation to all attacks that the use of such remote attack capabilities becomes lawful. This has been broadly achieved and demonstrated in respect of remotely piloted missions. Clearly, as the opening paragraphs of this article demonstrate, there are occasions when errors are made, but the making of errors does not call into question the lawfulness of the method of warfare as such. Rather, it is whether the method is capable of being employed in accordance with established legal requirements that is the critical issue under weapons law.[38]

As the previous section made clear, in certain narrowly defined generic circumstances autonomous attacks are also capable of being conducted in accordance with the requirements of the law of armed conflict. In the cyber domain, however, much will depend on the particular cyber tool that it is planned to use, on the characteristics of that tool, on whether the damaging effect of the cyber tool can be reasonably limited to the intended target of attack, and on whether enough is known about the target computer system to enable proper precautionary judgements of the sort discussed above to be made.

API requires that 'in the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by [API] or by any other rule of international law applicable to the High Contracting Party'.[39] Having concluded that cyber capabilities that are to be used to cause death, injury, damage or destruction to an opposing party to a conflict are means of warfare for the purposes of Article 36, it is clear that a legal review of such capabilities will be required and that the matters discussed in the previous paragraph will need to be considered when deciding whether the capability is indiscriminate by nature.[40]

38 For a discussion of the application of the law of armed conflict to cyber operations, see Charles J. Dunlap, 'Perspectives for cyber strategists on law for cyberwar', in *Strategic Studies Quarterly*, Spring 2011, pp. 81–99.

39 Article 36 of API.

40 W. H. Boothby, above note 37, pp. 69–85 and 345–347.

Liability considerations

Liability for error in remote attack

Legal discussion of remote attack technologies often centres on the question of responsibility. Who is responsible when something goes wrong? In the case of cyber attacks it may be very difficult to determine who precisely undertook the attack and with what particular purpose. The computer from which the attack was initiated may in some cases be identifiable, but the name of the person who created the cyber weapon, the name of the potentially different person who sent the cyber weapon on its way and the state, group, or other entity for which these persons were acting may never be known or capable of public disclosure. These difficulties may therefore make it impossible in practice to fix liability in the case of particular cyber events.

Responsibility, and the related notion of liability, can arise in differing contexts, including at the political/diplomatic level, in the media, at international law, and in domestic law. It may take the form of individual, including command, or state responsibility.

Media coverage of an incident may inform, or drive, perceived political responsibility for the event, as indeed political appreciations may influence media coverage. Early media reports, which may be based in whole or in part on flawed information, speculation, and assumption, and the responses thereto, may fix in the public mind a perception of responsibility that may be hard later to dispel if more reliable data come to light. Early disclosure by governments of factual data, including imagery, may be critical here. This implies, in policy terms, a need to have relevant information readily available in disclosable form if states are to engage successfully in the modern information and media campaigns. Responsibility tends to be attributed by the media to states, but if evidence of individual wrongdoing emerges within the period of active press interest the relevant persons may also attract critical media comment.

When it comes to attributing legal responsibility, judgements after the event must be based on the information, from all sources, that was reasonably available to the decision-maker at the relevant time.[41] In the case of an attack using a remotely piloted vehicle, the decision by the platform controller to undertake that attack will have been informed by the data fed to him when he was considering and making that decision. The vital issue will be whether that controller's decision to attack was reasonable in the circumstances as they were presented to him. Relevant questions may include whether there were any additional practicable precautions that were not taken and that, if taken, would have verified the status of the target as a military objective, whether the attack could be expected to be proportionate and whether it was being undertaken so as to minimize civilian injury and damage.[42]

41 See statement (c) made by the UK on ratification of API on 28 January 1998.

42 Note in this regard the observation in the UK Manual that the level at which legal responsibility to take precautions in attack rests is not specified in API, that whether a person has this responsibility will depend on whether he has any discretion as to the way in which the attack is carried out, and that the responsibility will therefore range from Commanders in Chief and their planning staffs to individual

It follows that if the relevant equipment was operating properly,[43] the operator of the platform is liable for his actions in relation to that platform. However, if for example the data feeds to the controller were adversely affected by a system fault, and if that fault can properly be said to have caused the erroneous decision to attack, then the system failure is likely to exonerate the controller from responsibility for the attack.

Similarly, if the opposing party to the conflict, whether through ruses, perfidy, voluntary or involuntary human-shielding or otherwise, materially impedes the platform operator's task, that will also be a factor to take into account when determining responsibility for the resulting events. It would not seem to be reasonable to lay blame at the door of the operator for errors attributable to the supporting systems, enemy action or other causes beyond his control. Whether the erroneous attack truly was beyond the operator's control will, however, be a question of fact to be assessed when all relevant information is available. It would seem that the factors to consider when determining potential liability of the controller of a remote platform are essentially similar to those that apply, for example, in the case of a pilot undertaking a similar mission.

There is no war crime of failing to take precautions in attack. Relevant war crimes under the Rome Statute, for example, would include directing attacks at civilians,[44] directing attacks at civilian objects[45] and prosecuting disproportionate attacks.[46] The intent that is an ingredient of these offences is not of course to be equated with a failure to take the required precautions, although in particular factual circumstances such a failure may be an element in such an intentional attack. Command responsibility would also be determined on a similar basis to that applying in relation to more conventional military operations, for example bombardment from piloted aircraft. A military commander is criminally responsible under the Rome Statute for crimes committed by forces under his or her effective command and control as a result of his or her failure to exercise control properly over such forces. The provision requires that either the military commander knew, or in the circumstances at the time should have known, that the forces were committing or about to commit such crimes and that he or she failed to take 'all necessary and reasonable measures within his or her power to repress or

soldiers opening fire on their own initiative; those carrying out orders for an attack must cancel or suspend it if the object to be attacked is such that the proportionality rule will be breached. *UK Joint Service Manual of the Law of Armed Conflict*, UK Ministry of Defence, 2004, para. 5.32.9.

43 This is an important caveat – opposing forces may be deliberately corrupting the image, impeding the operation of critical sensors, or using spoofs or other ruses to distort the picture.

44 Article 8(2)(b)(i) of the Rome Statute of the International Criminal Court, 1998 (hereinafter 'Rome Statute') provides for the crime of 'intentionally directing attacks against the civilian population as such or against individual civilians not taking direct part in hostilities'.

45 Article 8(2)(b)(ii) of the Rome Statute provides for the offence of 'intentionally directing attacks against civilian objects, that is, objects that are not military objectives'.

46 Article 8(2)(b)(iv) of the Rome Statute provides for the offence of 'intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects or wide-spread, long-term and severe damage to the natural environment which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated'.

prevent their commission'.[47] While the failure being discussed in the present article, namely the failure to take adequate precautions, does not amount to a war crime under the Rome Statute, any argument that commanders are also responsible for the failure is likely to be assessed according to similar criteria. Ultimately, the issue will be whether the commander knew, or ought to have known, that the method of attack being adopted precluded taking required precautions. It seems most likely that commanders would be aware of this.

Liability for lawful attacks

Generally speaking there is no liability at law for action by the armed forces of one party to an international armed conflict that lawfully causes death, injury, damage or destruction to an opposing party to the conflict.[48] To be lawful, such action must comply with the law of international armed conflict. Thus there is no liability for the damage lawfully done to military objectives, for the death or injury lawfully caused to members of the opposing armed forces, for expected death, injury or damage to civilians or civilian objects which is not excessive in relation to the anticipated concrete and direct military advantage, or for the death or injury of civilians or damage to civilian objects caused by mistaken or erroneous attacks caused, for example, by the malfunction of military equipment.

The liability to compensate provided in Article 3 of Hague Convention IV, 1907[49] is repeated in similar terms in Article 91 of API.[50] Applying Article 91, it would therefore seem that if, as a result of the failure to take all feasible precautions in relation to a remote attack operation, the attack causes excessive death or injury to civilians or excessive damage or destruction to civilian objects in relation to the concrete and direct military advantage anticipated there is likely to be a legal liability to compensate the affected civilians or civilian institutions if the case so demands. The API Commentary suggests that a simple violation of the law of armed conflict is not sufficient, that there must have been loss or damage and that compensation will only be appropriate if restitution in kind or the restoration of the pre-existing position is not possible.[51] This would suggest that, in order to establish liability, the claimants would need to prove that legally required precautions were not

47 Article 87 of API, and Article 28 of the Rome Statute.

48 The lawfulness of the action precludes liability of the state that undertook the attack in question; Hague Convention IV, Article 3, requires that there has been a violation. As to liability of individual combatants, Article 43(2) of API provides that members of the armed forces are combatants, that is they have the right to participate directly in hostilities.

49 The Article provides: 'A belligerent party which violates the provisions of the said Regulations shall, if the case so demands, be liable to pay compensation. It shall be responsible for all acts committed by persons forming part of its armed forces'.

50 This Article is in similar terms to Article 3 of Hague Convention IV, 1907, save that Article 91 refers to breaches of any of the 1949 Conventions or of the Protocol, and thus explicitly refers to breaches of the targeting rules in API. Paragraph 3646 of the *API Commentary* makes the point that the provision in Article 3 corresponded to the general principles of law on state responsibility, a view which is endorsed by the International Law Commission (ILC) in its *Commentary* to Article 7 of the Draft Articles on State Responsibility, 2001, para. 4.

51 For a more detailed discussion of compensatory arrangements, see *API Commentary*, paras 3652–3659.

taken,[52] that the claimants have suffered loss meriting the award of compensation, that this loss was caused by the failure to take precautions[53] and that the case demands the award of compensation.

If the injury to civilians and/or damage to civilian objects was caused by a technical malfunction of the equipment, such as faulty software, a manufacturing defect or the erroneous insertion of data during mission preparation, complex issues are likely to confront any attempt to ascribe individual responsibility. Military personnel who act negligently will be subject to their military discipline code, while available action against negligent civilians will depend on their employment contract. If, however, the error that has occurred is such that the incident cannot properly be described as a violation, the law of armed conflict will not require the payment of compensation.[54] Specifically, it would seem difficult to characterize the negligent manufacture of weaponry as a violation such as to form the basis for a possible claim for compensation under Article 91.[55] Whether in a particular case a claim would lie under product liability law would depend on the terms of the particular legislation of the relevant state and on the ability of the claimants to bring the claim within the jurisdiction of that state's civil law courts. Such issues lie outside the scope of the present article.

Does remote attack amount to a legally significant change in the conduct of warfare?

Remoteness of attack would be legally significant were it to render rules of targeting inoperable, or to render it impossible to allocate criminal responsibility for

52 Note, for example, the decision of the Eritrea-Ethiopia Claims Commission, partly based on adverse inferences, reinforcing the conclusion that not all feasible precautions were taken by Eritrea in its conduct of air strikes on Mekele on 5 June 1998 and finding Eritrea liable for the resulting deaths and injury to civilians and damage to civilian objects, reflected in Eritrea-Ethiopia Claims Commission, Partial Award Decision, *Central Front, Ethiopia's Claim 2*, 28 April 2004, para. 112, available at: http://www.pca-cpa.org/showpage.asp?pag_id=1151.

53 'Compensation can only be awarded in respect of damages having a sufficient causal connection with conduct violating international law . . . The degree of connection may vary depending upon the nature of the claim and other circumstances'; Eritrea-Ethiopia Claims Commission, *Decision Number 7*, para. 7, available at: http://www.pca-cpa.org/showpage.asp?pag_id=1151. Later in the same decision, the Commission determined that the necessary connection is best characterized as 'proximate cause' and that in deciding whether that test is met the Commission would consider whether the relevant event should have been reasonably foreseen by an actor committing the international delict in question; *ibid.*, para. 13. It would be for an adjudicating court, tribunal, or commission to determine, in the light of its remit, whether a similar approach should be adopted in determining whether a sufficient causal relationship exists between a failure to take precautions and ensuing injury, damage, or loss.

54 Compensatory payment may, however, be made on an *ex gratia* basis, such as reportedly occurred following the attack of the Chinese Embassy in Belgrade by US aircraft operating with NATO on 7 May 1999; see Kerry Dumbaugh, 'Chinese Embassy bombing in Belgrade: compensation issues', in *CRS* Report for Congress, available at: http://congressionalresearch.com/RS20547/document.php.

55 See T. Gillespie and R. West, above note 31, citing A. Myers, 'The legal and moral challenges facing the 21st century Air Commander', in *Royal Air Force Air Power Review*, Vol. 10, No. 1, Spring 2007, pp. 76–96, for the view that the responsibility of designers is discharged 'once the UAS [unmanned aerial system] has been certified by the relevant national air authority'; T. Gillespie and R. West, *ibid.*, p. 7.

wrongful acts or to adjudge whether compensation is payable for attacks that have unsatisfactory consequences.

There are, as we have seen, kinds of remote attack that do not pose such challenges. Thus, when a remotely piloted aerial vehicle is used to attack a target, the role of the remote pilot, usually referred to as the operator, mirrors that of a pilot of a manned aircraft such that targeting law rules can be applied in the same or a similar way, such that criminal liability could lie against the operator, say, in respect of a deliberate attack on civilians and compensation liability could be assessed and decided upon as in the case of an attack using a manned platform.

Moreover, in a sense, man has sought to fight from a distance since the earliest times. Concerns as to the ethics of such developments also date from ancient history.[56] The trebuchet, cannon, crossbow and longbow, artillery, bombardment from the air, and remotely piloted UAVs can all be regarded as technologically more refined methods of delivering offensive force against the enemy while incurring relatively less risk for one's own forces. This notion of seeking to protect oneself while placing the enemy at enhanced risk is of course central to many methods of warfare, which suggests that remoteness of the operator, per se, does not constitute a qualitative, and thus legally significant, change from what has gone before.[57] Perhaps the common thread here is that responsibility for attack decisions could always be readily ascribed at the personal, command and national levels. There will frequently be complications, for example where personnel from one nation on detached duty undertake attacks using platforms belonging to a state other than their own, either within a coalition or otherwise;[58] but those complications do not alter the fact that the person who ordered the attack, and the individuals who carried it out, can be identified and thus responsibility in the senses discussed in this article can be ascribed. Increasing the distance between the attacking individual and the scene where the destruction occurs does not, of itself, seem to change that. Rather, the issue seems to have more to do not so much with distance as with depersonalization altogether.

The anonymity or potential anonymity of a cyber attacker, the impossibility for the affected party to establish whose wrongful act caused an autonomous platform, say, to attack a civilian compound instead of a military objective, are examples of the sorts of circumstances in which we can say that these forms of remote attack would be starting to pose challenges for the law of targeting.

So let us consider autonomous attack technology a little further. If the platform belongs to and is operated by the armed forces of a state, that state will, it is suggested, have similar responsibility for what that piece of equipment does in the

56 The criticism by Idomeneus of the bow was that 'my way is not to fight my battles standing far away from my enemies'; Homer, *Illiad*, 13.262–3. O'Connell comments that the bow did not fit with the confrontational image that was the essence of heroic warfare; Robert L. O'Connell, *Of Arms and Men: A History of War, Weapons and Aggression*, Oxford University Press, Oxford, 1989, p. 48. Perhaps our ethical misgivings about some aspects of remote warfare have their origins in the Homeric notion of heroic warfare.

57 B. J. Strawser, above note 31, p. 343.

58 See Article 6 of the ILC Draft Articles on State Responsibility, 2001, available at: http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf, and note para. 3 of the associated commentary.

battle space to its responsibility for the death, injury or damage caused, for example, by a missile or bomb fired using more conventional, manned technology. In other words, Article 91 of API will determine whether there is a legal obligation to compensate, and the state will retain the discretion whether to make an *ex gratia* payment in circumstances where no legal liability can be, or has been, established.

Some may seek to conclude from this that if, for whatever reason, a platform autonomously decides to make civilians or civilian objects the object of attack that would prima facie constitute a breach of, respectively, Articles 51(2) or 52(1) of API and would thus constitute a violation for the purposes of Article 91. The alternative view, which the author prefers, would take into account the design of the controlling software, the data fed into the mission control equipment, the settings applied to the algorithm-based technology, and any other information that would demonstrate what the persons planning and commanding the mission intended that the machine should attack. According to this alternative view, the 'object' of an autonomous attack consists of the object(s) and/or person(s) that the target recognition equipment was designed or intended to engage. According to this latter view, the machine is using its autonomous capability to achieve the object, or purpose, set for it by those individuals in charge of the mission, with the implication that liability to compensate will only be established under Article 91 if it can be shown that those planners and commanders had as their object of attack the protected persons or objects.

Where personal responsibility for erroneous autonomous attack is concerned, it would seem sensible to conclude that individuals will generally be responsible for their own actions in relation to the autonomous platform, its navigation, and its offensive operation.[59] If an individual were deliberately to configure the autonomous target acquisition software with the intention that the platform would target civilians and/or civilian objects, it follows that that would amount to a war crime in just the same way as using conventional capabilities with a similar intent would be.[60] If a failure to take required precautions, however, causes an erroneous autonomous attack a war crime is unlikely to be established; compensation may be payable if the requirements for establishing liability under Article 91 can be established; and individuals responsible for the failure to take precautions may be disciplined, for example on the basis of negligent performance of duties, to the extent this is provided for in applicable armed forces discipline legislation or in the contract of civilian employment.

Conclusion

The tentative conclusion that emerges from this discussion is that the established framework, whether in respect of war crimes, liability to compensate or domestic armed forces or civilian employment discipline, should be capable of being applied,

59 Consider, however, paragraph 5.32.9 of the UK Manual summarized above at note 42.
60 Whether proceedings on such a basis would be viable would, as always, depend on the available evidence.

and therefore ought in fact to be applied, in the event of erroneous autonomous attacks. Persons who, in an international armed conflict, use autonomous technology deliberately to undertake unlawful attacks thereby breach the law of armed conflict as do those who use more conventional weaponry to like purpose. The fact that a machine is designed to act autonomously does not absolve those who give orders for the mission, those who plan the mission and those who take the necessary steps to enable the mission to be undertaken of responsibility for their own actions, and it is in the actions of those individuals that the basis for any criminality and liability to compensate is likely to be found.

Suggestions that criminal proceedings be taken against the machine are currently grounded in fiction. However, as notions of artificial intelligence (AI) continue to mature, it is conceivable that a point will arise at which human involvement is so remote, in a causal sense, from the decision to attack that commanders and planners can no longer sensibly be held accountable. In the author's view, we have not got to that point yet, but as technology becomes more complex and as decision-making relies increasingly on AI and less and less on human perception and judgement, the focus for responsibility may be expected to shift from planners and commanders to software engineers and the robots they beget.

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

Pandora's box? Drone strikes under *jus ad bellum*, *jus in bello*, and international human rights law

Stuart Casey-Maslen*

Dr Stuart Casey-Maslen is Head of Research at the Geneva Academy of International Humanitarian Law and Human Rights, specializing in weapons law and compliance with international norms by armed non-state actors.

Abstract

Armed drones pose a major threat to the general prohibition on the inter-state use of force and to respect for human rights. On the battlefield, in a situation of armed conflict, the use of armed drones may be able to satisfy the fundamental international humanitarian law rules of distinction and proportionality (although attributing international criminal responsibility for their unlawful use may prove a significant challenge). Away from the battlefield, the use of drone strikes will often amount to a violation of fundamental human rights. Greater clarity on the applicable legal regime along with restraints to prevent the further proliferation of drone technology are urgently needed.

Keywords: armed conflict, direct participation in hostilities, drone, human rights, international humanitarian law, law enforcement, targeted killing, unmanned aerial vehicle.

* The author would like to thank Professor Andrew Clapham, Professor Nils Melzer, and Bonnie Docherty for their comments on a draft of this article, and Alice Priddy for her background research. All the Internet references were accessed in October 2012, unless otherwise stated.

doi:10.1017/S1816383113000118

> Some have called such operations 'assassinations'. They are not, and the use of that loaded term is misplaced. Assassinations are unlawful killings.
>
> US Attorney General, Eric Holder, 5 March 2012[1]

Over the last ten years, the use of drones – unmanned aerial vehicles (UAVs) or unmanned aircraft[2] – for military and counterterrorism purposes has seen 'explosive growth'.[3] For example, it is reported that in 2010, United States President Barack Obama's administration authorized more than twice as many drone strikes in north-west Pakistan than it did in 2009 – 'itself a year in which there were more drone strikes than during George W. Bush's entire time in office'.[4] By early 2012, the Pentagon was said to have 7,500 drones under its control, representing about one-third of all US military aircraft.[5] Use of UAVs by police forces in connection with traditional law enforcement within a state's borders has also been steadily growing, albeit at a lesser pace.[6]

Drones[7] were first deployed on a significant scale for surveillance and reconnaissance in armed conflict by the United States of America: in Vietnam in

1 Speech to the Northwestern University School of Law, Chicago, 5 March 2012, available at: http://www.lawfareblog.com/2012/03/text-of-the-attorney-generals-national-security-speech/.

2 According to US Federal legislation adopted in 2012, the term 'unmanned aircraft' means 'an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft'. Section 331(8), FAA Modernization and Reform Act of 2012, signed into law by the US President on 14 February 2012.

3 US Department of Defence, 'US unmanned systems integrated roadmap (fiscal years 2009–2034)', Washington, DC, 2009, p. 2, available at: http://www.acq.osd.mil/psa/docs/UMSIntegratedRoadmap2009.pdf. Presumably no pun was intended.

4 Peter Bergen and Katherine Tiedemann, 'Hidden war, there were more drone strikes – and far fewer civilians killed', in *New America Foundation*, 22 December 2010, available at: http://newamerica.net/node/41927.

5 W. J. Hennigan, 'New drone has no pilot anywhere, so who's accountable?', in *Los Angeles Times*, 26 January 2012, available at: http://www.latimes.com/business/la-fi-auto-drone-20120126,0,740306.story. A similar percentage of drones to piloted aircraft is expected within twenty years in the British Royal Air Force (RAF). Nick Hopkins, 'Afghan civilians killed by RAF drone', in *The Guardian*, 5 July 2011, available at: http://www.guardian.co.uk/uk/2011/jul/05/afghanistan-raf-drone-civilian-deaths. General N. A. Schwartz, the US Air Force Chief of Staff, has reportedly deemed it 'conceivable' that drone pilots in the Air Force would outnumber those in cockpits in the foreseeable future, although he predicted that the US Air Force would have traditional pilots for at least thirty more years. Elisabeth Bumiller, 'A day job waiting for a kill shot a world away', in *The New York Times*, 29 July 2012, available at: http://www.nytimes.com/2012/07/30/us/drone-pilots-waiting-for-a-kill-shot-7000-miles-away.html?pagewanted=all.

6 See, e.g., 'Groups concerned over arming of domestic drones', in *CBSDC*, Washington, DC, 23 May 2012, available at: http://washington.cbslocal.com/2012/05/23/groups-concerned-over-arming-of-domestic-drones/; Vincent Kearney, 'Police in Northern Ireland consider using mini drones', in *BBC*, 16 November 2011, available at: http://www.bbc.co.uk/news/uk-northern-ireland-15759537; BBC, 'Forces considering drone aircraft', 26 November 2009, available at: http://news.bbc.co.uk/2/hi/uk_news/england/8380796.stm; Ted Thornhill, 'New work rotor: helicopter drones to be deployed by US police forces for the first time (and it won't be long before the paparazzi use them, too)', in *Daily Mail*, 23 March 2012, available at: http://www.dailymail.co.uk/sciencetech/article-2119225/Helicopter-drones-deployed-U-S-police-forces-time-wont-long-paparazzi-use-too.html. The US Federal Aviation Authority Modernization and Reform Act of 2012 grants increased powers to local police forces across the USA to use their own drones.

7 According to the Oxford English Dictionary, the pertinent definition of a drone is 'a remote-controlled pilotless aircraft or missile', the etymology being the Old English word for a male bee. In Pakistan, the drones, which make a buzzing noise, are nicknamed *machay* (wasps) by the Pashtuns. Jane Meyer, 'The

the 1960s,[8] in Bosnia and Herzegovina, and Kosovo in the 1990s.[9] Most recently, in 2012, it has been reported that drones have been used by the Syrian regime to identify the location of rebel forces.[10] But although they are used in this role (and some armed forces use them only for this), they are better known for firing explosive weapons in targeted killings[11] of suspected 'terrorists', especially in cross-border operations.

At the same time as scientific developments are leading to larger and faster drones, miniaturization has been paving the way for UAVs the size of insects – 'nano' drones[12] – that could also be used for targeted killings, possibly using poison. In February 2011, researchers unveiled a prototype hummingbird drone, which can fly at 11 miles per hour and perch on a windowsill.[13]

Robotic warfare is also on the horizon, with its obvious difficulties for establishing individual criminal responsibility (which are discussed below). In this regard, a media report in 2011 warned that fully autonomous drones, able to determine a target and fire on it without a 'man in the loop' (that is, independent of human control after launch), were being prepared for deployment by the USA,[14] potentially representing the greatest challenge to *jus in bello* since the development of chemical warfare.[15] In an internal study of drones published by the UK Ministry of Defence in 2011, it was asserted that: 'In particular, if we wish to allow systems to make independent decisions without human intervention, some considerable

Predator war', in *The New Yorker*, 26 October 2009, http://www.newyorker.com/reporting/2009/10/26/091026fa_fact_mayer.

8 David Cenciotti, 'The dawn of the robot age: US Air Force testing air-launched UCAVs capable to fire Maverick and Shrike missiles in 1972', in *The Aviationist* (weblog), 14 March 2012, available at: http://theaviationist.com/2012/03/14/the-dawn-of-the-robot-age/.

9 'Predator drones and unmanned aerial vehicles (UAVs)', in *The New York Times*, updated 5 March 2012, available at: http://topics.nytimes.com/top/reference/timestopics/subjects/u/unmanned_aerial_vehicles/index.html.

10 'Syrian forces use drone in attack on rebel city', in *ABC News*, 12 June 2012, available at: http://www.abc.net.au/news/2012-06-12/52-killed-in-syria-as-troops-pound-rebels-strongholds/4064990.

11 According to Alston, a targeted killing is 'the intentional, premeditated and deliberate use of lethal force, by States or their agents acting under colour of law, or by an organized armed group in armed conflict, against a specific individual who is not in the physical custody of the perpetrator'. Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston, Addendum, Study on targeted killings, Report to the Human Rights Council, UN Doc. A/HRC/14/24/Add.6, 28 May 2010, para. 1, available at: http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf (hereinafter, 2010 Study on Targeted Killings). Melzer affirms that a targeted killing has five cumulative elements: use of lethal force; intent, premeditation, and deliberation to kill; targeting of individually selected persons; lack of physical custody; and the attributability of the killing to a subject of international law. Nils Melzer, *Targeted Killings in International Law*, Oxford Monographs in International Law, Oxford University Press, Oxford, 2008, pp. 3–4.

12 J. Meyer, above note 7.

13 Elisabeth Bumiller and Thom Shanker, 'War evolves with drones, some tiny as bugs', in *The New York Times*, 19 June 2011, available at: http://www.nytimes.com/2011/06/20/world/20drones.html?pagewanted=1&_r=1&ref=unmannedaerialvehicles.

14 W. J. Hennigan, 'New drone has no pilot anywhere, so who's accountable?', in *Los Angeles Times*, 26 January 2012, http://www.latimes.com/business/la-fi-auto-drone-20120126,0,740306.story.

15 Emma Slater, 'UK to spend half a billion on lethal drones by 2015', *The Bureau of Investigative Journalism*, 21 November 2011, available at: http://www.thebureauinvestigates.com/2011/11/21/britains-growing-fleet-of-deadly-drones/.

work will be required to show how such systems will operate legally'.[16] Similarly, the US Department of Defense affirmed in 2009 that:

> Because the Department of Defence complies with the Law of Armed Conflict, there are many issues requiring resolution associated with employment of weapons by an unmanned system. . . . For a significant period into the future, the decision to pull the trigger or launch a missile from an unmanned system will not be fully automated, but it will remain under the full control of a human operator. Many aspects of the firing sequence will be fully automated but the decision to fire will not likely be fully automated until legal, rules of engagement, and safety concerns have all been thoroughly examined and resolved.[17]

Given that drones are clearly 'here to stay'[18] – indeed, 'killer drones' are said by a former CIA lawyer to be 'the future of warfare'[19] – this article looks at the legality of UAV strikes within and across borders,[20] and within both armed conflict and situations of law enforcement. It will thus address the interplay between *jus ad bellum, jus in bello*, and the rules governing law enforcement, especially international human rights law. It ends with a brief discussion of the future challenges to international law from the use of armed drones and robots.

Before embarking on more detailed discussion, however, it is worth recalling Article 36 of the 1977 Additional Protocol I, which requires that:

> In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.

As a new method of warfare, the delivery of missiles by pilotless aircraft controlled by operators – often civilians – stationed thousands of miles away should already have been subjected to rigorous scrutiny by those states seeking to develop or procure drones. At the very least, the obligation set out in Article 36 should encompass all states that are party to the 1977 Additional Protocol I, although,

16 Development, Concepts and Doctrine Centre, *The UK Approach to Unmanned Aircraft Systems*, Joint Doctrine Note 2/11, Ministry of Defence, 2011, p. 5–2, para. 503. The report further stated that: 'Estimates of when artificial intelligence will be achieved (as opposed to complex and clever automated systems) vary, but the consensus seems to lie between more than 5 years and less than 15 years, with some outliers far later than this.' *Ibid.*, p. 5–4, para. 508.

17 US Department of Defence, above note 3, p. 10.

18 See E. Bumiller and T. Shanker, above note 13. According to the US Department of Defense, 'Unmanned systems will continue to have a central role in [the US's] diverse security needs, especially in the War on Terrorism'. US Department of Defence, above note 3, p. iii.

19 Afsheen John Radsan, 'Loftier standards for the CIA's remote-control killing', Statement for the House Subcommittee on National Security & Foreign Affairs, in *Legal Studies Research Paper Series, Accepted Paper No. 2010–11*, William Mitchell College of Law, St Paul, Minnesota, May 2010, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1604745.

20 Other aspects of the use of drones, such as surveillance and reconnaissance, will not be assessed in this article.

INTERNATIONAL REVIEW of the Red Cross

arguably, the general obligation to 'respect and to ensure respect' for international humanitarian law (IHL) should incite every state, whether or not it is party to the Protocol, to conduct such legal analysis.[21] However, the seventy or more states that reportedly possess drones have not made public their own analysis – if they have conducted one – of the legality of armed drones, whether for use in armed conflict or for law enforcement purposes.[22]

Drones and *jus ad bellum*

Jus ad bellum governs the legality of recourse to military force, including through drone strikes, by one state against another and against armed non-state actors in another state without that latter state's consent.[23] Under Article 2, paragraph 4 of the UN Charter,

> [a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

Cryer *et al.* describe this as the 'fundamental legal principle governing the use of force', which 'reflects customary international law'.[24] However, as is also well known, under Article 51 of the Charter it is stipulated that:

> Nothing in the present Charter shall impair the inherent right of collective or individual self-defence if an armed attack occurs against a member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security.[25]

21 Somewhat surprisingly, the International Committee of the Red Cross (ICRC)'s study of customary IHL published in 2005 did not find that Article 36 was part of the corpus of customary law, seemingly due to a lack of positive state practice. Notwithstanding this lacuna, it is hard to understand how customary obligations prohibiting the use of indiscriminate weapons or of weapons of a nature to cause superfluous injury or unnecessary suffering (respectively Rules 71 and 70 of the ICRC study) can be respected unless a weapon's capabilities are first tested by legal analysis to ensure that they comply with the law. See Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law*, ICRC and Cambridge University Press, 2005. The USA, for instance, not a state party to the Protocol, conducts detailed reviews of weapons prior to their deployment. See, e.g., US Department of Defence, above note 3, p. 42.

22 See, e.g., Peter Bergen and Jennifer Rowland (New America Foundation), 'A dangerous new world of drones', in *CNN*, 1 October 2012, available at: http://newamerica.net/node/72125. Indeed, it was only in early 2012, ten years after the first drone strike, that the US administration formally acknowledged the existence of its covert programme for the use of armed drones. In an online Google+ and YouTube chat on 31 January 2012, President Obama said the strikes targeted 'people who are on a list of active terrorists'. See, e.g., www.youtube.com/watch?v=2TASeH7gBfQ, posted by *Al Jazeera* on 31 January 2012.

23 Thus, as Lubell observes, the *jus ad bellum* framework is not designed to restrict the use of force within a state's own borders. Noam Lubell, *Extraterritorial Use of Force against Non-State Actors*, Oxford Monographs in International Law, Oxford University Press, Oxford, 2011, p. 8.

24 Robert Cryer, Hakan Friman, Darryl Robinson and Elizabeth Wilmshurst, *An Introduction to International Criminal Law and Procedure*, 2nd edn, Cambridge University Press, Cambridge, 2010, p. 322.

25 UN Charter, Art. 51. Aside from self-defence and use of force authorized by the UN Security Council, it is only lawful to use force in another state with that state's consent.

The definition of an armed attack in the case of armed groups armed and equipped by a foreign state was elaborated on by the International Court of Justice (ICJ) in the *Nicaragua* case as follows:

> The Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces. But the Court does not believe that the concept of 'armed attack' includes not only acts by armed bands where such acts occur on a significant scale but also assistance to rebels in the form of the provision of weapons or logistical or other support. Such assistance may be regarded as a threat or use of force, or amount to intervention in the internal or external affairs of other States.[26]

The threshold for the occurrence of an armed attack by another state thus appears to be relatively high, going beyond 'a mere frontier incident' between members of the armed forces of two states (or armed groups operating in one state with limited support from another state). It might even be argued by some that a very limited and targeted drone strike by one state against individuals located in another state would not constitute an armed attack in the sense of the UN Charter or customary law, with the argument being based on the highly contested concept of anticipatory self-defence.[27] Nevertheless, in the absence of lawful self-defence such use of armed force would undoubtedly contravene the general prohibition on the use or threat of force (and therefore amount to a violation of international law unless the use of force was consented to by the 'victim' state).[28] Almost certainly, a more intensive cross-border use of drone strikes, akin to a bombardment, would be an armed attack on another state and therefore constitute aggression, absent Security Council authorization or being an action being taken in legitimate self-defence.[29]

However, there is a strong argument that even one drone strike constitutes an armed attack and potentially aggression. Indeed, UN General Assembly Resolution 3314 (XXIX) provided that an act of aggression shall be constituted, inter alia, by: 'Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State'.[30] The 1988 case of nine Israeli commandos killing a single Palestine Liberation Organization military strategist in his home in Tunis, which the UN Security Council condemned as an 'aggression' in flagrant violation of the UN Charter, further supports the argument.[31]

26 International Court of Justice (ICJ), *Case concerning Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua* v. *United States of America*), Judgment, 27 June 1986, para. 195.
27 See, e.g., Antonio Cassese, *International Law*, 2nd edn, Oxford University Press, Oxford, 2005, pp. 357–363.
28 For details of the conditions for the lawful granting of consent, see, e.g., *ibid.*, pp. 370–371.
29 See, e.g., *ibid.*, pp. 158–159.
30 UN General Assembly Resolution 3314 (XXIX) of 14 December 1974, Annex, Art. 3(b).
31 UN Security Council Resolution 611 (1988), adopted on 25 April 1988 by fourteen votes with one abstention (USA).

If a single drone strike does constitute an 'armed attack', the state launching the drone will need to justify its action by reference to its inherent right of self-defence (unless it had received the requisite consent or an authorization from the UN Security Council); otherwise it would be at risk of committing an act of aggression.[32] The situation is controversial when self-defence is claimed not against another state but against an armed non-state actor located in another state. In its 2004 Advisory Opinion in the *Wall* case, the ICJ appeared to imply that self-defence could only be invoked by one state against another state.[33] A closer reading of the dicta, though, suggests that the ICJ did not entirely rule out the possibility of self-defence against an armed non-state actor that commits 'terrorist' acts where effective control was not exercised by the state under threat.[34] In the subsequent *Case Concerning Armed Activities on the Territory of the Congo*, the ICJ avoided the question as to whether international law allows for self-defence 'against large-scale attacks by irregular forces'.[35] A separate, minority opinion by Judge Kooijmans in this case goes further than the *Wall* dicta, asserting that:

> if the attacks by the irregulars would, because of their scale and effects, have had to be classified as an armed attack had they been carried out by regular armed forces, there is nothing in the language of Article 51 of the Charter that prevents the victim State from exercising its *inherent* right of self-defence.[36]

The traditional customary law governing self-defence by a state derives from an early diplomatic incident between the USA and the UK over the killing of a number of US citizens engaged in transporting men and materials from American territory to support rebels in what was then the British colony of Canada.[37] Under the so-called Caroline test, for a lawful right to self-defence there must exist 'a necessity

32 An act of aggression is generally defined as the use of armed force by one state against another state without the justification of self-defence or authorization by the UN Security Council. The actions qualifying as acts of aggression are explicitly influenced by UN General Assembly Resolution 3314 (XXIX) of 14 December 1974. Under Article 8 *bis* of the 1998 Rome Statute of the International Criminal Court, as adopted by the First Review Conference in Kampala in 2010, the individual crime of aggression is the planning, preparation, initiation, or execution by a person in a leadership position of an act of aggression. Such an act must constitute a 'manifest violation' of the UN Charter (Article 8 *bis*, para. 1).

33 ICJ, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 2004, para. 139.

34 The Court (para. 139) refers to UN Security Council resolutions 1368 (2001) and 1373 (2001), passed in the aftermath of the 11 September 2001 attacks against the USA, noting that 'Israel exercises control in the Occupied Palestinian Territory and that, as Israel itself states, the threat which it regards as justifying the construction of the wall originates within, and not outside, that territory. The situation is thus different from that contemplated by Security Council resolutions 1368 (2001) and 1373 (2001), and therefore Israel could not in any event invoke those resolutions in support of its claim to be exercising a right of self-defence'. In both instances, a preambular paragraph to the respective resolution recognises 'the inherent right of individual or collective self-defence in accordance with the Charter'.

35 ICJ, *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo* v. *Uganda)*, 19 December 2005, para. 147.

36 *Ibid*., Separate Opinion of Judge Kooijmans, para. 29.

37 See in this regard, Christopher Greenwood, 'International law and the pre-emptive use of force: Afghanistan, Al-Qaida, and Iraq', in *San Diego International Law Journal*, Vol. 4, 2003, p. 17; and N. Lubell, above note 23, p. 35; and Andrew Clapham, *Brierly's Law of Nations*, 7th edn, Oxford University Press, Oxford, 2008, pp. 468–469.

of self-defence, instant, overwhelming, leaving no choice of means, and no moment of deliberation' and, furthermore, any action taken must be proportional, 'since the act justified by the necessity of self-defence must be limited by that necessity, and kept clearly within it'.[38] These statements in 1842 by the US Secretary of State to the British authorities are widely accepted as an accurate description of a state's customary right of self-defence.[39]

Therefore, the two principles of necessity and proportionality must both be met if the use of force by a state claiming to be acting in self-defence is to be adjudged lawful. Failure to meet the twin criteria means that the use of force may even constitute aggression. In its 1996 Advisory Opinion on the *Legality of the Threat or Use of Nuclear Weapons*, the ICJ stated that the two interdependent requirements constitute a rule of customary international law.[40] According to the principle of necessity, 'the State attacked (or threatened with imminent attack if one admits preventive self-defence) must not, in the particular circumstances, have had any means of halting the attack other than recourse to armed force'.[41] The principle of proportionality, on the other hand, is rather more abstruse, for despite the word generally connoting a balancing (often of contrary concepts), its intent in this context is rather different:

> The requirement of proportionality of the action taken in self-defence … concerns the relationship between that action and its purpose, namely … that of halting and repelling the attack … It would be mistaken, however, to think that there must be proportionality between the conduct constituting the armed attack and the opposing conduct. The action needed to halt and repulse the attack may well have to assume dimensions disproportionate to those of the attack suffered. … Its lawfulness cannot be measured except by its capacity for achieving the desired result. In fact, the requirements of the 'necessity' and 'proportionality' of the action taken in self-defence can simply be described as two sides of the same coin.[42]

This viewpoint, particularly the claim that effectiveness in stopping an armed attack is determinant of proportionality,[43] has been addressed indirectly in

38 Letter dated 27 July 1842 from Mr Webster, US Department of State, Washington, DC, to Lord Ashburton.

39 See, e.g., A. Clapham, above note 37, pp. 469–470.

40 'As the Court stated in the case concerning Military and Paramilitary Activities in and against Nicaragua (*Nicaragua* v. *United States of America*), there is a 'specific rule whereby self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it, a rule well established in customary international law'. The Court noted that this dual condition 'applies equally to Article 51 of the Charter, whatever the means of force employed'. ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion of 8 July 1996, para. 41.

41 'Addendum – Eighth report on State responsibility by Mr Roberto Ago, Special Rapporteur – the internationally wrongful act of the State, source of international responsibility (part 1)', Extract from the *Yearbook of the International Law Commission 1980*, Vol. II(1), UN Doc. A/CN.4/318/Add.5-7, para. 120.

42 *Ibid*., para. 121.

43 See, e.g., Elizabeth Wilmshurst, 'Principles of international law on the use of force by states in self-defence', Chatham House Working Paper, October 2005, esp. pp. 7–8, 10, available at: http://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/ilpforce.doc.

other ICJ jurisprudence. In the 2003 *Oil Platforms* case (*Iran* v. *USA*), the Court concluded that:

> As to the requirement of proportionality, the attack of 19 October 1987 might, had the Court found that it was necessary in response to the *Sea Isle City* incident as an armed attack committed by Iran, have been considered proportionate. In the case of the attacks of 18 April 1988, however, they were conceived and executed as part of a more extensive operation entitled 'Operation Praying Mantis'. . . . As a response to the mining, by an unidentified agency, of a single United States warship, which was severely damaged but not sunk, and without loss of life, neither 'Operation Praying Mantis' as a whole, nor even that part of it that destroyed the Salman and Nasr [oil] platforms, can be regarded, in the circumstances of this case, as a proportionate use of force in self-defence.[44]

Both the application and the precise threshold for the lawful use of force in self-defence remain uncertain.[45] Nonetheless, it is arguably the case that a state that uses an armed drone in a cross-border operation, which has not been consented to by the state on whose territory the 'terrorist' is located, may only legitimately claim it was acting in self-defence if the threat or use of force against it amounts to an armed attack.[46] A threat of an isolated, more limited 'terrorist' attack would therefore not be sufficient. This has potentially significant implications, in particular, for the use of armed drones by Israel on Palestinian territory. In any event, it would also appear, based on Article 51 of the UN Charter, that the use of an armed drone by a state against another or in another's territory purporting to be in self-defence must at least be immediately reported to the Security Council if it is to be lawful.[47] This is not known to have happened yet.[48]

44 ICJ, *Case Concerning Oil Platforms, Islamic Republic of Iran* v. *United States of America*, Judgment of 6 November 2003, para. 77.

45 Including with respect to claims of a right to self-defence that arises from low-level, cumulative attacks by non-state actors. See in this regard, Special Rapporteur '2010 study on targeted killings', above note 11, para. 41.

46 As Alston has asserted, 'it will only be in very rare circumstances that a non-state actor whose activities do not engage the responsibility of any State will be able to conduct the kind of armed attack that would give rise to the right to use extraterritorial force'. Special Rapporteur '2010 study on targeted killings', above note 11, para. 40.

47 'Measures taken by members in exercise of this right of self-defence shall be immediately reported to the Security Council'. Alston goes further, arguing that the UN Charter would require that Security Council approval should be sought. *Ibid*., para. 40.

48 Moreover, even when operating in a state that appears on the facts – and despite regular public pronouncements to the contrary – to implicitly at least acquiesce to the use of drones on its territory, the fact of using drones to target 'terrorists' is certainly not popular. In an interview with Voice of America (VOA) on 31 January 2012, a Pakistani Foreign Ministry spokesman called the US missile strikes 'illegal, counterproductive and unacceptable, and in violation of Pakistan's sovereignty' even though it is asserted that they are carried out with the help of Pakistani intelligence. 'Obama's drone strikes remark stirs controversy', in *VOA*, 31 January 2012, available at: http://www.voanews.com/content/pakistan-repeats-condemnation-of-drone-strikes-138417439/151386.html.

Drones and international humanitarian law

Potentially, the use of drones on the battlefield is relatively uncontroversial under *jus in bello* (without prejudice to *jus ad bellum*) because there may be scant practical difference between the use of a Cruise missile or an aerial bombardment and the use of a drone equipped with explosive weapons.[49] Indeed, according to the UN Special Rapporteur on extrajudicial, summary or arbitrary executions, although 'in most circumstances targeted killings violate the right to life, in the exceptional circumstance of armed conflict, they may be legal'.[50] Whether or not the use of armed drones constitute aggression or legitimate self-defence, should they take place within a situation of armed conflict and fulfil the relevant nexus criteria (see below subsection on the nexus to the conflict) they will also be judged under applicable *jus in bello*, particularly IHL.[51] They will thus have to comply with, at a minimum, the IHL rules applicable to the conduct of hostilities, in particular those rules relating to precautions in attacks, distinction, and proportionality, and they must not employ weapons the use of which is unlawful under IHL. These rules are discussed in turn.

Precautions in attacks

There are direct links between respect for the rules on precautions in attacks and respect for other customary rules applicable to the conduct of hostilities, notably distinction (discrimination) and proportionality, as well as the prohibition on using means or methods of warfare that are of a nature to cause superfluous injury or unnecessary suffering. Most of the rules on precautions in attacks, which were codified in 1977 Additional Protocol I, are of a customary nature and are applicable in non-international armed conflict as well as in international armed conflict, according to the International Committee of the Red Cross (ICRC) study published in 2005. Central among the rules is the obligation to take 'constant care' in the conduct of military operations to 'spare the civilian population, civilians, and civilian objects'. In this regard, '[a]ll feasible precautions must be taken to avoid, and in any event to minimise, incidental loss of civilian life, injury to civilians, and damage to civilian objects'.[52] Article 57 of the Protocol provides that those who plan

49 US drones have been actively deployed in Afghanistan since 2001; it has been claimed that the first-ever drone strike occurred during the November 2001 invasion, targeting a high-level Al Qaeda meeting in Kabul. See, e.g., John Yoo, 'Assassination or targeted killings after 9/11', in *New York Law School Law Review*, Vol. 56, 2011/12, p. 58, citing also James Risen, 'A nation challenged: Al Qaeda; Bin Laden aide reported killed by US bombs', in *The New York Times*, 17 November 2001, p. A1, available at: http://www.nytimes.com/2001/11/17/world/a-nationchallenged-al-qaeda-bin-laden-aide-reported-killed-by-us-bombs.html. From April 2011, drone strikes were also used in the armed conflict in Libya where they famously struck the convoy carrying the deposed leader Muammar al-Gaddafi out of Sirte in October of the same year.

50 '2010 study on targeted killings', above note 11, para. 10.

51 Thus, acts that are unlawful under *jus in bello* would not necessarily constitute disproportionate responses for the purposes of determining the legality of actions taken in self-defence under *jus ad bellum*.

52 ICRC's Study on customary international humanitarian law, above note 21, Rule 15.

or decide upon an attack shall 'take all feasible precautions in the choice of means and methods of attack'.[53]

For several reasons it could be argued that drone strikes might fulfil the requirements for precautions in attacks. First, a video feed from the drone can give 'real-time' eyes on the target so that the absence of civilians close to the target can be monitored until the last few minutes or even seconds.[54] Second, it appears that at least some of the targets of drone strikes are located using a tracking device that is presumably attached (or 'painted' on) to the vehicle, luggage, or equipment, or even potentially the person or one of the persons being targeted. Third, in certain cases (notably on Afghan soil), nearby military forces are also charged with monitoring the target. Fourth, other than the thermobaric variant of the Hellfire missile,[55] most of the missiles fired from drones are believed to have a smaller blast radius than other conventional munitions that might typically be deployed from a fighter jet. These factors do not eliminate the risk of civilian casualties, but they certainly represent feasible precautions that can minimize incidental loss of civilian life.[56]

Significant failings have undeniably occurred, however, with one drone strike in Afghanistan in 2010 alone killing twenty-three Afghan civilians and wounding twelve others.[57] In May 2010, the US military released a report on the deaths, saying that 'inaccurate and unprofessional' reporting by Predator drone operators had led to the airstrike in February 2010 on the group of civilian men, women, and children.[58] The report said that four American officers, including

53 1977 Additional Protocol (AP) I, Art. 57(2)(a)(ii).

54 In contrast, an unnamed former White House counterterrorism official has reportedly asserted that '"there are so many drones" in the air over Pakistan that arguments have erupted over which remote operators can claim which targets, provoking "command-and-control issues"'. See J. Meyer, above note 7.

55 According to one US defence industry website, the AGM-114N variant of the Hellfire uses a thermobaric (metal augmented charge) warhead that can suck the air out of a cave, collapse a building, or produce 'an astoundingly large blast radius out in the open'. 'US Hellfire missile orders, FY 2011-2014', in *Defense Industry Daily*, 10 January 2012, available at: http://www.defenseindustrydaily.com/US-Hellfire-Missile-Orders-FY-2011-2014-07019/.

56 Though, note the caution expressed in this regard by Alston: 'Drones' proponents argue that since drones have greater surveillance capability and afford greater precision than other weapons, they can better prevent collateral civilian casualties and injuries. This may well be true to an extent, but it presents an incomplete picture. The precision, accuracy and legality of a drone strike depend on the human intelligence upon which the targeting decision is based'. '2010 study on targeted killings', above note 11, para. 81. Indeed, as Daniel Byman has argued: 'To reduce casualties, superb intelligence is necessary. Operators must know not only where the terrorists are, but also who is with them and who might be within the blast radius. This level of surveillance may often be lacking, and terrorists' deliberate use of children and other civilians as shields make civilian deaths even more likely'. Daniel L. Byman, 'Do targeted killings work?', in *Brookings Institution*, 14 July 2009, available at: http://www.brookings.edu/opinions/2009/0714_targeted_killings_byman.aspx.

57 'First drone friendly fire deaths', in *RT*, 12 April 2011, available at: http://rt.com/usa/news/first-drone-friendly-fire/. In October 2011, the US Department of Defense concluded that a number of miscommunication errors between military personnel had led to a drone strike the previous April, a strike that mistakenly killed two US troops in Afghanistan. 'Drone strike killed Americans', in *RT*, 17 October 2011, available at: http://rt.com/usa/news/drone-american-military-report-057/.

58 Dexter Filkins, 'Operators of drones are faulted in Afghan deaths', in *The New York Times*, 29 May 2010, available at: http://www.nytimes.com/2010/05/30/world/asia/30drone.html. The report, signed by Major-General T. P. McHale, found that the Predator operators in Nevada and 'poorly functioning command posts' in the area failed to provide the ground commander with evidence that there were civilians in the trucks. According to military officials in Washington and Afghanistan, who spoke on the condition of

a brigade and battalion commander, had been reprimanded, and that two junior officers had also been disciplined. General Stanley A. McChrystal, who apologized to Afghan President Hamid Karzai after the attack, announced a series of training measures intended to reduce the chances of similar events. General McChrystal also asked Air Force commanders to open an investigation into the Predator operators.[59]

The question of how many civilians are killed in drone strikes is highly polarized.[60] It was reported in *The New York Times* in May 2012 that the Obama administration had embraced a method for counting civilian casualties that 'in effect counts all military-age males in a strike zone as combatants … unless there is explicit intelligence posthumously proving them innocent'.[61] Seen in the light of these events, the 'extraordinary claim' in June 2011 by President Obama's top counterterrorism adviser, John O. Brennan, that there had not been 'a single collateral death' over the previous twelve months is of highly questionable accuracy.[62]

The rule on distinction

With respect to the rule on distinction, which can be considered the most fundamental of all IHL rules, its application in an international armed conflict is far simpler than it is in an armed conflict of a non-international character. Use of drone strikes appears to have been confirmed in only two international armed conflicts to date, namely the USA and others against Afghanistan (the Taliban – as opposed to Al Qaeda[63] – forces) in 2001–2002[64] and the one that pitted NATO member states' armed forces against Libya in 2011. It is, however, also likely that drone strikes were

anonymity, intelligence analysts who were monitoring the drone's video feed sent computer messages twice, warning the drone operators and ground command posts that children were visible.

59 *Ibid.*

60 See, e.g., Chris Woods, 'Analysis: CNN expert's civilian drone death numbers don't add up', in *The Bureau of Investigative Journalism,* 17 July 2012, available at: http://www.thebureauinvestigates.com/2012/07/17/analysis-cnn-experts-civilian-drone-death-numbers-dont-add-up/.

61 Jo Becker and Scott Shane, 'Secret "kill list" proves a test of Obama's principles and will', in *The New York Times*, 29 May 2012, available at: http://www.nytimes.com/2012/05/29/world/obamas-leadership-in-war-on-al-qaeda.html?_r=1&pagewanted=all.

62 'The Bureau of Investigative Journalism, which monitors the toll, counted "credible media accounts" of between 63 and 127 non-militant deaths in 2011, and a recent Associated Press investigation found evidence that at least 56 villagers and tribal police had been killed in the 10 largest strikes since August 2010. But analysts, American officials and even many tribesmen agree the drones are increasingly precise. Of 10 strikes this year, the local news media have alleged civilian deaths in one case. The remainder of those killed – 58 people, by conservative estimates – were militants'. Declan Walsh, Eric Schmitt and Ihsanullah T. Mehsud, 'Drones at issue as US rebuilds ties to Pakistan', in *The New York Times*, 18 March 2012, available at: http://www.nytimes.com/2012/03/19/world/asia/drones-at-issue-as-pakistan-tries-to-mend-us-ties.html?pagewanted=all. For a robust defence of drone strikes and claims that the number of civilian casualties is greatly exaggerated, see, e.g., Gregory S., McNeal , 'Are targeted killings unlawful? A case study in empirical claims without empirical evidence', in C. Finkelstein, J. D. Ohlin and A. Altmann (eds), *Targeted Killings, Law and Morality in an Asymmetrical World*, Oxford University Press, Oxford, 2012, pp. 326–346.

63 In the view of the author, the combat with Al Qaeda in Afghanistan since 2001 is best classified as a separate, non-international armed conflict.

64 The conflict against the Taliban changed in character as a result of the *Loya Jirga* that in June 2002 elected President Hamid Karzai. With respect to the qualification of the armed conflicts in Afghanistan, see, e.g.,

conducted in 2003–2004 during the attack against Iraq,[65] which formed part of the international armed conflict between the USA (and others) against the regime of Saddam Hussein.

These examples aside, it is clear that the overwhelming majority of drone strikes during armed conflict have occurred in conflicts that are non-international in character: by the USA and the UK in Afghanistan from June 2002;[66] and by the USA in Pakistan,[67] Somalia,[68] and Yemen.[69] In Iraq, unarmed drones are today being used by the US Department of State for surveillance purposes only;[70] armed drones were also used there in the past, with controversial effect.[71] In India, drones are employed to help Indian Special Forces to home in on Maoist fighters, but the UAVs they use are said to be unarmed.[72]

Given these realities, the applicable rule on distinction – between lawful military objectives and civilians and civilian objects – is typically that which governs the conduct of hostilities in armed conflicts of a non-international character. Only lawful military targets, including civilians 'participating directly in hostilities', may lawfully be targeted by attacks, in accordance with the provisions of Common Article 3 to the four Geneva Conventions, as supplemented by customary international law (and, where applicable, Art. 13(3) of 1977 Additional Protocol II).[73]

Robin Geiß and Michael Siegrist, 'Has the armed conflict in Afghanistan affected the rules on the conduct of hostilities?', in *International Review of the Red Cross*, Vol. 93, No. 881, March 2011, especially. pp. 13 ff.

65 See, e.g., 'Unmanned aerial vehicles (UAVs)', in *GlobalSecurity.org*, last modified 28 July 2011, available at: http://www.globalsecurity.org/intell/systems/uav-intro.htm.

66 Australia and Canada are believed to use unarmed Heron drones. See, e.g., 'Canada, Australia contract for Heron UAVs', in *Defense Industry Daily*, 17 July 2011, available at: http://www.defenseindustrydaily.com/Canada-Contracts-for-Heron-UAVs-05024/.

67 See, e.g., 'US drone strike kills "16" in Pakistan', in *BBC*, 24 August 2012, http://www.bbc.co.uk/news/world-asia-19368433.

68 The first drone strike against al-Shabaab forces is believed to have taken place in late June 2011. Declan Walsh, 'US begins drone strikes on Somalia militants', in *The Guardian*, 1 July 2011, p. 18.

69 See, e.g., Ahmed Al Haj, 'Khaled Batis dead: US drone strike in Yemen reportedly kills top Al Qaeda militant', in *Huffington Post*, 2 September 2012, available at: http://www.huffingtonpost.com/2012/09/02/khaled-batis-dead_n_1850773.html; and Hakim Almasmari, 'Suspected US drone strike kills civilians in Yemen, officials say', in *CNN*, 4 September 2012, available at: http://edition.cnn.com/2012/09/03/world/meast/yemen-drone-strike/index.html.

70 Eric Schmitt and Michael S. Schmidt, 'US drones patrolling its skies provoke outrage in Iraq', in *The New York Times*, 29 January 2012, available at: http://www.nytimes.com/2012/01/30/world/middleeast/iraq-is-angered-by-us-drones-patrolling-its-skies.html?pagewanted=all.

71 J. Meyer, above note 7.

72 Nishit Dholabhai, 'Scanner in sky gives fillip to Maoist hunt', in *The Telegraph* (India), Calcutta, 16 January 2012, available at: http://www.telegraphindia.com/1120117/jsp/nation/story_15015539.jsp.

73 The USA is not a State Party to the Protocol, although Afghanistan is. Even were the USA to adhere to the Protocol, it might argue that based on Article 1 of the Protocol this instrument would apply only to Afghanistan and/or would exclude its extraterritorial application to attacks in Pakistan. This is because under its Article 1, the Protocol applies 'to all armed conflicts … which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol.' For a better view on the applicability of the Protocol in Afghanistan to, at least, all states parties to that instrument, see, e.g., the Rule of Law in Armed Conflicts (RULAC) project, Australia profile, Qualification of Armed Conflicts section, especially note 2, available at: http://www.geneva-academy.ch/RULAC/applicable_international_law.php?id_state=16.

The ICRC's *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* is highly controversial in certain respects. No one appears to claim that IHL prohibits targeting the armed forces of a state that is party to a non-international armed conflict.[74] Far more controversial is the assertion that (military) members of organized armed groups that are a party to such a conflict likewise fulfil the requisite criteria on the basis of a claimed 'continuous combat function'.[75] Those who exercise such a continuous combat function may, in principle, be targeted by attacks at any time (though this general permissiveness is subject to the rule on military necessity). As Alston observes:

> the creation of CCF [continuous combat function] category is, *de facto*, a status determination that is questionable given the specific treaty language that limits direct participation to 'for such time' as opposed to 'all the time.' . . . Creation of the CCF category also raises the risk of erroneous targeting of someone who, for example, may have disengaged from his or her function.[76]

A further challenge is how to identify – legally and practically – who such military members are. As the *Interpretive Guidance* published by the ICRC observes:

> under IHL, the decisive criterion for individual membership in an organized armed group is whether a person assumes a continuous function for the group involving his or her direct participation in hostilities (hereafter: 'continuous combat function'). . . . [This function] distinguishes members of the organized fighting forces of a non-State party from civilians who directly participate in hostilities on a merely spontaneous, sporadic, or unorganized basis, or who assume exclusively political, administrative or other non-combat functions.[77]

Those who directly participate in hostilities on a merely spontaneous, sporadic, or unorganized basis may only lawfully be targeted while they so participate (although at other times they may of course be arrested by a law enforcement operation and charged under domestic law for offences committed). Those who assume exclusively political, administrative, or other non-combat functions may not be lawfully targeted unless and until they directly participate in hostilities, and only for such

74 See Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, ICRC, Geneva, 2009, pp. 30–31 (hereinafter, *ICRC Interpretive Guidance*).

75 See *ibid.*, pp. 27–28. 'The term organized armed group . . . refers exclusively to the armed or military wing of a non-State party: its armed forces in a functional sense'. *Ibid.*, p. 32.

76 '2010 study on targeted killings', above note 11, paras. 65–66.

77 *ICRC Interpretive Guidance*, above note 74, p. 33. According to Melzer, continuous combat function 'may also be identified based on conclusive behaviour, for example where a person has repeatedly directly participated in hostilities in support of an organized armed group in circumstances indicating that such conduct constitutes a continuous function rather than a spontaneous, sporadic, or temporary role assumed for the duration of a particular operation'. *Ibid.*, p. 35; and see N. Melzer, 'Keeping the balance between military necessity and humanity: a response to four critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation In Hostilities', in *New York University Journal of International Law and Politics*, Vol. 42, 2010, p. 890 (hereinafter, 'Keeping the balance').

time as they undertake such acts.[78] In case of doubt as to his or her status, a person should be considered a civilian not directly participating in hostilities.[79]

On this basis, using lethal force to target an Al Qaeda operative in Afghanistan who is engaged in planning, directing, or carrying out an attack in Afghanistan against, for example, US forces, would therefore be, a priori, lawful under the IHL rule of distinction. Targeting his son, his daughter, his wife, or wives would not be lawful, unless (and only for such time as) they were directly participating in hostilities.[80] The legality of an attack against the operative, where the attack was also expected to incidentally kill or injure civilians, would depend on a determination according to the rule of proportionality (see below subsection on proportionality in attacks).

Failing to make such a distinction during attack would render the attack unlawful and constitute evidence of a war crime.[81] In March 2012, the UK law firm Leigh Day & Co and the charity Reprieve launched an action against British foreign secretary William Hague on behalf of Noor Khan, whose father Malik Daud Khan

78 In contrast, Brigadier-General Watkin proposes to significantly widen the category of those who would fall within the definition, notably including persons assuming exclusively 'combat service support' functions, including cooks and administrative personnel. Kenneth Watkin, 'Opportunity lost: organized armed groups and the ICRC "Direct Participation in the Hostilities" Interpretive Guidance', in *New York University Journal of International Law and Politics*, Vol. 42, 2010, p. 692, available at: http://www.law.nyu.edu/ecm_dlv1/groups/public/@nyu_law_website__journals__journal_of_international_law_and_politics/documents/documents/ecm_pro_065932.pdf. See N. Melzer, 'Keeping the balance', above note 77, pp. 848–849.

79 According to Recommendation VIII of the ICRC's *Interpretive Guidance*: 'All feasible precautions must be taken in determining whether a person is a civilian and, if so, whether that civilian is directly participating in hostilities. In case of doubt, the person must be presumed to be protected against direct attack'. *ICRC Interpretive Guidance*, above note 74, pp. 75–76. See also N. Melzer, 'Keeping the balance', above note 77, especially pp. 874–877. Radsan asserts that: 'Except in extraordinary circumstances, the agency may strike only if it is satisfied beyond a reasonable doubt that its target is a functional combatant of al Qaeda or a similar terrorist group. Drone strikes, in effect, are executions without any realistic chance for appeal to the courts through habeas corpus or other procedures'. A. J. Radsan, above note 19, p. 3. Regrettably, he later claims that: 'There are, of course, exceptions to my general rule for CIA targeting. I summarize these exceptions under the label of extraordinary circumstances. The target, for example, may play an irreplaceable role in al Qaeda. A drone operator may see a person on the screen who is probably Bin Laden – but not Bin Laden beyond any doubt. Even so, the military advantage of killing Bin Laden, compared to a mid-level terrorist, may justify the additional risk of mistakenly harming a peaceful civilian'. (*Ibid.*, p. 5.)

80 In this regard, Melzer notes the USA's understanding, declared in the context of the Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict, that 'the phrase "direct part in hostilities": (i) means immediate and actual action on the battlefield likely to cause harm to the enemy because there is a direct causal relationship between the activity engaged in and the harm done to the enemy; and (ii) does not mean indirect participation in hostilities, such as gathering and transmitting military information, transporting weapons, munitions, or other supplies, or forward deployment'. See N. Melzer, 'Keeping the balance', above note 77, p. 888, and note 226.

81 In this regard, claims that numerous CIA drone strikes have targeted funerals or those rescuing the victims of drone strikes are extremely disquieting. According to a report by the Bureau of Investigative Journalism: 'A three-month investigation including eye witness reports has found evidence that at least 50 civilians were killed in follow-up strikes when they had gone to help victims. More than 20 civilians have also been attacked in deliberate strikes on funerals and mourners'. Chris Woods and Christina Lamb, 'Obama terror drones: CIA tactics in Pakistan include targeting rescuers and funerals', in *Bureau of Investigative Journalism*, 4 February 2012, available at: http://www.thebureauinvestigates.com/2012/02/04/obama-terror-drones-cia-tactics-in-pakistan-include-targeting-rescuers-and-funerals/.

was killed in a drone strike in Pakistan in 2011 'while presiding over a peaceful council of tribal elders'.[82]

In 2009, it was reported in the media that the US Department of Defense's Joint Integrated Prioritized Target List – the Pentagon's roster of approved terrorist targets, containing 367 names – had been expanded to include some fifty Afghan drug lords suspected of giving money to help finance the Taliban.[83] Individuals engaged in the cultivation, distribution, and sale of narcotics are, a priori, criminals; however, even if they willingly or otherwise finance terrorism, they are not directly participating in hostilities in Afghanistan.[84] Targeting individual criminals with drone strikes would therefore be unlawful.

The rule of proportionality

Even if a target is a lawful military objective under IHL the question of proportionality arises and may either affect the selection of the means and methods of warfare that may lawfully be used, or even effectively prohibit an attack being launched. Violating the rule of proportionality is an indiscriminate attack according to 1977 Additional Protocol I.[85] The rule is not given voice in either Common Article 3 to the Geneva Conventions or 1977 Additional Protocol II, but is deemed to be a customary rule of IHL applicable not only in international armed conflict but also in armed conflicts of a non-international character. According to Rule 14 of the ICRC's study of customary international humanitarian law:

> Launching an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated, is prohibited.

The question, of course, is what is 'excessive'? In the ICRC-published commentary on Article 51(5) of the 1977 Additional Protocol I, from where the text setting out the rule on proportionality in attack originates, it is stated that:

> Of course, the disproportion between losses and damages caused and the military advantages anticipated raises a delicate problem; in some situations there will be no room for doubt, while in other situations there may be reason for hesitation. In such situations the interests of the civilian population should prevail.[86]

82 'GCHQ staff could be at risk of prosecution for war crimes', in *Gloucester Echo*, 13 March 2012, available at: http://www.thisisgloucestershire.co.uk/GCHQ-staff-risk-prosecution-war-crimes/story-15505982-detail/story.html.

83 J. Meyer, above note 7.

84 See, in this regard, '2010 study on targeted killings', above note 11, para. 68.

85 See 1977 AP I, Art. 51(5)(b) and Art. 57(2)(a)(iii).

86 Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols*, ICRC, Geneva, 1987, paras. 1979–1980.

It is well known that different states have widely differing assessments of what is proportionate. Even close military allies, such as the UK and the USA, appear to differ materially on this issue. An instructive example occurred in Afghanistan in March 2011 when a UK Royal Air Force drone killed four Afghan civilians and injured two others in an attack against 'insurgent leaders' in Helmand province, the first confirmed operation in which a UK Reaper aircraft had been responsible for the death of civilians.[87] According to a press report, the UK Ministry of Defence spokesman said:

> Any incident involving civilian casualties is a matter of deep regret and we take every possible measure to avoid such incidents. On 25 March a UK Reaper was tasked to engage and destroy two pick-up trucks. The strike resulted in the deaths of two insurgents and the destruction of a significant quantity of explosives being carried on the trucks. Sadly, four Afghan civilians were also killed and a further two Afghan civilians were injured. There are strict procedures, frequently updated in light of experience, intended to both minimise the risk of casualties occurring and to investigate any incidents that do happen.

An ISAF investigation was conducted to establish if any lessons could be learnt from the incident or if errors in operational procedures could be identified; the report noted that the UK Reaper's crews' actions had been in accordance with procedures and UK Rules of Engagement.[88]

Nonetheless, a 'source', apparently from the UK Ministry of Defence, informed the British *Guardian* newspaper that the attack 'would not have taken place if we had known that there were civilians in the vehicles as well'.[89] Thus, while the target (that is to say, individual insurgents in at least one of the pick-up trucks) would probably not have been unlawful under IHL, it seems that the UK would have considered it disproportionate to target the two insurgents had they had known that the civilians were present.

Contrast this example with the case of the Taliban leader, Baitullah Mehsud. On 23 June 2009, the CIA killed Khwaz Wali Mehsud, a mid-ranking Pakistan Taliban commander. They planned to use his body as 'bait' to target Baitullah Mehsud, who was expected to attend Khwaz Wali Mehsud's funeral. Up to 5,000 people attended the funeral, including not only Taliban fighters but many civilians. US drones struck again, killing up to eighty-three people. Forty-five of the dead were reportedly civilians, among them ten children and four tribal leaders. Such an attack raises very serious questions about respect for the prohibition on indiscriminate attacks. Baitullah Mehsud escaped unharmed, reportedly dying six weeks later, along with his wife, in another CIA attack.[90]

87 N. Hopkins, above note 5.
88 *Ibid.*
89 *Ibid.*
90 C. Woods and C. Lamb, above note 81. According to Meyer, the CIA conducted sixteen missile strikes with the deaths of up to 321 people before they managed to kill Baitullah Mehsud. See J. Meyer, above note 7.

The use of lawful weaponry

Customary law prohibits the use, whether in international or non-international armed conflicts, of inherently indiscriminate weapons, as well as of weapons that are of a nature to cause superfluous injury or unnecessary suffering.[91] In general, the Hellfire missiles typically fired from drones do not appear to violate this criterion.[92] As noted above, however, a cautionary note is warranted where potential use of thermobaric Hellfire missiles is concerned. Given their wide area effects and consequences for human beings, such thermobaric missiles demand further consideration under both general principles relating to weaponry.[93] Moreover, as drones are only platforms, other weapons can be – and are – used, which may fall foul of the rules prohibiting the use of unlawful weapons in armed conflict.

The nexus to the conflict

Are the strikes in Pakistan, specifically those against Al Qaeda suspects, to be considered legal conduct of hostilities within the armed conflict in Afghanistan?[94] In remarks online on 31 January 2012, President Obama said that the drone strikes in Pakistan, which are carried out by the CIA rather than the military,[95] are a 'targeted, focused effort at the people who are on a list of active terrorists' and that the USA was not just 'sending in a whole bunch of strikes willy-nilly' but targeting 'Al Qaeda suspects who are up in very tough terrain along the border between Afghanistan and Pakistan'.[96] A 'terrorist' is not, however, necessarily someone who is engaged in an armed conflict (let alone the even further removed case of drug lords noted above). There must be a clear nexus to an armed conflict with a clearly defined non-state party, not an ill-defined, globalized 'war against terror', especially since the current US administration has sought to distance itself from such rhetoric.[97] As Melzer has noted:

> Whether or not a group is involved in hostilities does not only depend on whether it resorts to organized armed violence temporally and geographically coinciding with a situation of armed conflict, but also on whether such violence

91 See the ICRC's study of customary IHL, above note 21, Rules 70 and 71.

92 Given that drone strikes often occur in populated areas, were the blast radius of missiles used to increase in size there would be greater concerns about compliance with the prohibition on indiscriminate attacks.

93 Thermobaric weapons are described as 'among the most horrific weapons in any army's collection: the thermobaric bomb, a fearsome explosive that sets fire to the air above its target, then sucks the oxygen out of anyone unfortunate enough to have lived through the initial blast'. Noah Shachtman, 'When a gun is more than a gun', in *Wired*, 20 March 2003, available at: http://www.wired.com/politics/law/news/2003/03/58094 (last visited on 20 February 2012, but page no longer online).

94 Where, in contrast, Pakistani or Afghani Taliban members are planning and conducting cross-border raids into Afghanistan, or the USA is conducting drone strikes in support of Pakistan's non-international armed conflict against the Pakistan Taliban (TTP), these are clearly related to a specific armed conflict.

95 The CIA drones are said to be controlled from a suburban facility near the Agency's headquarters in Langley, Virginia. See D. Walsh, above note 68.

96 See, e.g., 'Obama discusses US use of drones in online Q&A – video', in *The Guardian*, 31 January 2012, available at: http://www.guardian.co.uk/world/video/2012/jan/31/obama-us-drones-video.

97 See, e.g., N. Lubell, above note 23, pp. 113, especially note 5, and 114.

is designed to support one of the belligerents against another (belligerent nexus).[98]

According to the US Attorney General, Eric Holder, who addressed the issue of drone strikes in a speech in March 2012, the US government's 'legal authority is not limited to the battlefields in Afghanistan'. Mr Holder said there were circumstances under which 'an operation using lethal force in a foreign country, targeted against a US citizen who is a senior operational leader of Al Qaeda or associated forces, and who is actively engaged in planning to kill Americans, would be lawful'.[99] Such circumstances included that a thorough review had determined the individual posed 'an imminent threat of violent attack against the United States', that 'capture is not feasible', and the 'operation would be conducted in a manner consistent with applicable law of war principles'.[100]

While the limiting of legality of targeted killings to senior operational leaders of Al Qaeda or associated forces who pose 'an imminent threat of violent attack against the United States' might be welcome as it suggests that unless the threat of violent attack is 'imminent', an attack will not be authorized, it still raises a series of questions. First, what constitutes an 'imminent' threat? Second, many of those killed in drone strikes in Pakistan are not senior leaders but mid- or low-level fighters. Quid the legality of these strikes? Or do the criteria only restrict drone strikes when it concerns a US citizen? Is it 'open season' on foreign nationals?[101] Third, is an attack against US forces in Afghanistan by fighters based in Pakistan deemed a terrorist attack by the US government? Although the definition of terrorism remains highly controversial, many would argue that it is the targeting of civilians, not members of a state's armed forces, that is one of the defining characteristics of terrorism,[102] along with an associated attempt to influence government policy on one or more issues. This is clearly not, however, the US government's understanding of the term 'terrorism'.

And, again, the Attorney General's statement does not address the issue of whether such strikes form part of an armed conflict: an oral commitment to conduct an operation 'in a manner consistent with applicable law of war principles' does not mean that IHL is applicable under international law. The US Supreme Court, in *Hamdan v. Rumsfeld*, rejected the assertion that the conflict was a global war against Al Qaeda to which the Geneva Conventions did not apply, and

98 N. Melzer, 'Keeping the balance', above note 77, p. 841; see also N. Melzer, above note 11, p. 427.

99 The notion of 'associated forces' needs clarification. The USA would be on firmer legal ground if it publicly narrowed its list designated for killing to members of the Al Qaeda leadership, not anyone who publicly or privately supports their objectives or sympathizes with their methods.

100 'Attorney General Eric Holder defends killing of American terror suspects', in *Daily Telegraph*, 6 March 2012, available at: http://www.telegraph.co.uk/news/worldnews/al-qaeda/9125038/Attorney-General-Eric-Holder-defends-killing-of-American-terror-suspects.html.

101 As Radsan notes: 'If non-American lives are just as important as American lives, then one model of due process (or "precaution" to use an IHL term), should apply across the board. In negative terms, if the controls are not good enough for killing Americans, then they are not good enough for killing Pakistanis, Afghans, or Yemenis'. See A. J. Radsan, above note 19, p. 10.

102 See, e.g., UN, 'A more secure world: Our shared responsibility, Report of the High-level Panel on Threats, Challenges and Change', New York, 2004 (UN High Level Panel), paras. 159–161.

specifically determined that Common Article 3 to the Geneva Conventions applied to Salim Ahmed Hamdan, a former bodyguard and driver of Osama bin Laden, an individual who was captured by US military forces inside Afghanistan in November 2001.[103] This judgment does not mean that anyone – wherever he (or she) may be in the world – affiliated to Al Qaeda is drawn into an armed conflict of a non-international character against the USA as a person participating directly in hostilities by virtue of espousal of, or even indirect support for, a violent ideology.[104]

Drone strikes and international human rights law

The application and impact of IHL on drone strikes in a situation of armed conflict having been reviewed above, this section looks at the implications of international human rights law for the use of armed drones. The first targeted killing using a drone strike outside a theatre of armed conflict is believed to have been the killing of six alleged Al Qaeda members, including Qaed Senyan al-Harithi, also known as Abu Ali, who was the suspected mastermind of the bombing of the USS *Cole* in October 2000.[105] The six were killed on 3 November 2002 in Yemen when either one or two Hellfire missiles[106] launched from a drone controlled by the US Central Intelligence Agency (CIA) destroyed the jeep in which they were travelling in the northern Yemeni province of Marib, about 160 kilometres east of Sana'a.[107] Since then, targeted killings using drones have become a regular occurrence in Pakistan and, albeit to a lesser extent, in Yemen as well as in other countries.[108] The September 2011 killing, by a CIA drone, in Yemen of Anwar al-Awlaki, a radical Muslim cleric of Yemeni descent, was particularly controversial as he was

103 US Supreme Court, *Hamdan* v. *Rumsfeld*, 29 June 2006, pp. 67–69.

104 See, e.g., M. E. O'Connell, 'Seductive drones: learning from a decade of lethal operations', Notre Dame Legal Studies Paper No. 11-35, in *Notre Dame Law School Journal of Law, Information & Science*, August 2011; and as cited by Carrie Johnson, 'Holder spells out why drones target US citizens', in *NPR*, 6 March 2012, http://www.npr.org/2012/03/06/148000630/holder-gives-rationale-for-drone-strikes-on-citizens.

105 See N. Melzer, above note 11, p. 3; 'Sources: US kills Cole suspect', in *CNN*, 4 November 2002, available at: http://articles.cnn.com/2002-11-04/world/yemen.blast_1_cia-drone-marib-international-killers?_s=PM:WORLD.

106 The AGM-114 Hellfire is an air-to-surface missile developed primarily for anti-armour use, which can be launched from air, sea, or ground platforms. See, e.g., Lockheed Martin, 'HELLFIRE II Missile', in *Lockheed Martin* website, undated, available at: http://www.lockheedmartin.com/us/products/HellfireII.html (last visited 20 March 2012). The name of the missile, the first guided launch of which occurred in 1978, comes from its original conception as a helicopter-launched 'fire-and-forget' weapon (HELicopter Launched FIRE-and-forget). 'AGM-114A HELLFIRE missile', in *Boeing*, available at: http://www.boeing.com/history/bna/hellfire.htm.

107 See, e.g., 'CIA "killed al-Qaeda suspects" in Yemen', in *BBC*, 5 November 2002; and 'US Predator kills 6 Al Qaeda suspects', in *ABC News*, 4 November 2002, available at: http://abcnews.go.com/WNT/story?id=130027&page=1. According to the *ABC* news report, all that remained of the car 'was rubble in the desert'.

108 Israeli forces have conducted targeted killings of Palestinians using drones. See, e.g., 'Three killed in Israeli airstrike', in *CNN*, 1 April 2011, available at: http://articles.cnn.com/keyword/gaza-strip; 'Gaza truce gets off to a shaky start', in *CNN*, 23 June 2012, available at: http://articles.cnn.com/2012-06-23/middleeast/world_meast_israel-gaza-violence_1_gaza-truce-popular-resistance-committees-palestinian-medical-officials?_s=PM:MIDDLEEAST.

a US citizen.[109] After earlier failed drone strikes against him, his family had launched a legal challenge seeking to prevent the USA from executing one of its citizens without any judicial process.[110]

The first subsection below discusses how human rights law regulates the use of force outside armed conflict in a 'law enforcement' situation, while the second looks at its role and consequences – actual and potential – within armed conflict as a constituent of *jus in bello* alongside IHL.

Application of human rights law to law enforcement

Under international human rights law two important principles govern all use of force in a law enforcement setting: necessity and proportionality. Although these terms have been used in the context of both *jus ad bellum* and IHL, their precise meaning in the context of human rights law is markedly different. As Alston has stated: 'A State killing is legal only if it is required to protect life (making lethal force *proportionate*) and there is no other means, such as capture or nonlethal incapacitation, of preventing that threat to life (making lethal force *necessary*)'.[111] A further requirement is that the threat to life which the use of lethal force is seeking to forestall must be imminent.[112] Thus, in its approach to regulating the intentional use of lethal force, international human rights law generally embraces the standards laid down in the 1990 Basic Principles on the Use of Force and Firearms by Law Enforcement Officials (the 'Basic Principles').[113] According to the final sentence of Basic Principle 9: 'In any event, intentional lethal use of firearms may only be made when strictly unavoidable in order to protect life'.[114]

This general position is, however, subject to two caveats. First, the Basic Principles were not designed to regulate acts by armed forces in a situation of armed conflict, which remain under the purview of *jus in bello*. Second, the threshold for the intentional lethal use of force has been set less restrictively by domestic

109 'Predator drones and unmanned aerial vehicles (UAVs)', in *The New York Times*, updated 5 March 2012.

110 'Obituary: Anwar al-Awlaki', in *BBC,* 30 September 2011, available at: http://www.bbc.co.uk/news/world-middle-east-11658920.

111 '2010 study on targeted killings', above note 11, para. 32. As Melzer has noted, under the law enforcement 'paradigm', the 'proportionality test asks not whether the use of potentially lethal force is "necessary" to remove a concrete threat, but whether it is "justified" in view of the nature and scale of that threat'. N. Melzer, above note 11, p. 115.

112 According to Principle 9 of the 1990 Basic Principles on the Use of Force and Firearms by Law Enforcement Officials (emphasis added): 'Law enforcement officials shall not use firearms against persons except in self-defence or defence of others against the *imminent* threat of death or serious injury, to prevent the perpetration of a particularly serious crime involving grave threat to life, to arrest a person presenting such a danger and resisting their authority, or to prevent his or her escape, and only when less extreme means are insufficient to achieve these objectives'.

113 Adopted by the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, 27 August to 7 September 1990. The USA did not participate in this meeting, but a UN General Assembly resolution adopted the same year welcomed the Basic Principles and invited governments 'to respect them and to take them into account within the framework of their national legislation and practice'. UN General Assembly Resolution 45/166, A/45/PV.69, adopted without a vote on 18 December 1990, Operative Paragraph 4.

114 Principle 8 provides that: 'Exceptional circumstances such as internal political instability or any other public emergency may not be invoked to justify any departure from these basic principles'.

US jurisprudence (relating to police powers) and similarly interpreted more permissively by the Inter-American Commission on Human Rights (with respect to counterterrorism operations).[115] In *Tennessee v. Garner*,[116] the US Supreme Court stated that:

> Where the officer has probable cause to believe that the suspect poses a threat of serious physical harm, either to the officer or to others, it is not constitutionally unreasonable to prevent escape by using deadly force. Thus, if the suspect threatens the officer with a weapon or there is probable cause to believe that he has committed a crime involving the infliction or threatened infliction of serious physical harm, deadly force may be used if necessary to prevent escape, and if, where feasible, some warning has been given.[117]

Other nations, including Australia and the UK, support the higher standard as set out in the Basic Principles. For example, the UK has a shoot-to-kill policy for suspected suicide bombers, but which clearly meets that higher standard because a suicide bomber not only threatens death, but also is likely to meet the criterion of imminence that is an integral element accompanying the level of threat. Following the July 2005 killing by Metropolitan Police officers of an unarmed youth, Jean Charles de Menezes, wrongly suspected to be a suicide bomber and shot seven times at point-blank range,[118] Lord Stevens, the former Metropolitan Police Commissioner, made public – in a British tabloid newspaper – a policy that had been adopted when he was in charge in 2002.[119] He told that British newspaper that the teams he sent to Israel and other countries[120] hit by suicide bombers after

115 The Commission appears, however, to confuse the situations in which firearms may be used (imminent threat of death or serious injury) with those in which intentional lethal force may be employed. Indeed, in claiming that the use of lethal force by law enforcement officials is lawful also to protect themselves or other persons from imminent threat of serious injury, it cites Basic Principle 9, which as we have seen limits the intentional use of lethal force to where it is strictly unavoidable in order to protect life. Certain leading authors seem to have committed similar errors. See, e.g., N. Melzer, 'Keeping the balance', above note 77, p. 903; N. Melzer, , above note 11, pp. 62, 197; and N. Lubell, above note 23, p. 238.

116 *Tennessee* v. *Garner*, 471 US 1, Appeal from the US Court of Appeals for the Sixth Circuit, No. 83-1035 (27 March 1985). The case involved the fatal shooting by a police officer of an unarmed 15-year-old boy. The suspect, who was shot in the back of the head with a .38-calibre pistol loaded with hollow point bullets, was fleeing a suspected burglary. On his person was found money and jewellery worth $10 that he had allegedly taken from the house.

117 The Court cited with approval the model penal code whereby: 'The use of deadly force is not justifiable . . . unless (i) the arrest is for a felony; and (ii) the person effecting the arrest is authorized to act as a peace officer or is assisting a person whom he believes to be authorized to act as a peace officer; and (iii) the actor believes that the force employed creates no substantial risk of injury to innocent persons; and (iv) the actor believes that (1) the crime for which the arrest is made involved conduct including the use or threatened use of deadly force; or (2) there is a substantial risk that the person to be arrested will cause death or serious bodily harm if his apprehension is delayed'. American Law Institute, Model Penal Code, Section 3.07(2)(b) (proposed Official Draft 1962), cited in *Tennessee* v. *Garner, ibid.*, para. 166, note 7.

118 See, e.g., 'De Menezes police "told to shoot to kill"', in *Daily Telegraph*, 3 October 2007, available at: http://www.telegraph.co.uk/news/uknews/1564965/De-Menezes-police-told-to-shoot-to-kill.html. This incident shows the potential for fatal mistakes to be made even when round-the-clock, direct and indirect surveillance is maintained on a terrorist suspect.

119 The policy, codenamed Operation Kratos, was named after the Greek demi-god Kratos, meaning strength or power in ancient Greek.

120 Reportedly Russia and Sri Lanka.

the 11 September 2001 attacks in the USA had learned a 'terrible truth', that the only way to stop a suicide bomber was to 'destroy his brain instantly, utterly'. Previously, officers had fired at the offender's body, 'usually two shots, to disable and overwhelm'.[121] Sir Ian Blair, who was Commissioner in 2005, stated that there was 'no point' in shooting a suspect in the chest as that is where a bomb would most likely be and it would detonate.[122]

The question of imminence is extremely important to the issue of drone strikes, especially given the risk of subjectivity and lack of transparency as to who is on the US list of those designated for elimination.[123] The speech by Attorney General Holder in March 2012 appeared to seek to marry two different legal regimes – one applicable to a law enforcement paradigm and the other applicable to armed conflict – when he claimed that authorization for the use of a drone strike against a US citizen would require 'a thorough review' that had determined the individual posed 'an imminent threat of violent attack against the United States' and that 'capture is not feasible'. In 2010, Koh stated that:

> [it] is the considered view of this Administration – and it has certainly been my experience during my time as Legal Adviser – that US targeting practices, including lethal operations conducted with the use of unmanned aerial vehicles, comply with *all applicable law*, including the laws of war.[124]

In May 2012, *The New York Times* reported on the existence of 'Terror Tuesdays', when the US President would decide who would be killed by the USA, typically through drone strikes:

> This was the enemy, served up in the latest chart from the intelligence agencies: 15 Qaeda suspects in Yemen with Western ties. The mug shots and brief biographies resembled a high school yearbook layout. Several were Americans. Two were teenagers, including a girl who looked even younger than her 17 years.[125]

Given the significant constraints on the intentional use of lethal force under international human rights law, Alston concludes that: 'Outside the context of armed conflict, the use of drones for targeted killing is almost never likely to be legal. A targeted drone killing in a state's own territory, over which the State has control,

121 'Debate rages over "shoot-to-kill"', in *BBC,* 24 July 2005, available at: http://news.bbc.co.uk/1/hi/uk/4711769.stm. Lord Stevens said: 'We are living in unique times of unique evil, at war with an enemy of unspeakable brutality, and I have no doubt that now, more than ever, the principle is right despite the chance, tragically, of error. . . . And it would be a huge mistake for anyone to even consider rescinding it'.

122 The use of 'less-lethal' weapons, such as the Taser conducted electrical weapon, is also not recommended for fear it might detonate the explosives. See, e.g., Memorandum entitled 'Counter Suicide Terrorism' from the Clerk to the Metropolitan Police Authority to the Members of the MPA, London, 8 August 2005.

123 See '2010 study on targeted killings', above note 11, para. 20. There is also an obvious risk that targeted killings are seen as lethal retribution for past crimes. See, e.g., in Pakistan, N. Melzer, above note 11, p. 178.

124 Speech by Harold Hongju Koh, Legal Adviser, US Department of State, to the Annual Meeting of the American Society of International Law, Washington, DC, 25 March 2010 (emphasis added), available at: http://www.state.gov/s/l/releases/remarks/139119.htm.

125 J. Becker and S. Shane, above note 61.

would be very unlikely to meet human rights law limitations on the use of lethal force'. Furthermore, outside a state's own territory,

> there are very few situations outside the context of active hostilities in which the test for anticipatory self-defence … would be met. … In addition, drone killing of anyone other than the target (family members or others in the vicinity, for example) would be an arbitrary deprivation of life under human rights law and could result in state responsibility and individual criminal liability.[126]

For Lubell, for example, the killing of al-Harithi in Yemen in 2002 was unlawful on the basis that it violated the right to life as set out in the 1966 Covenant on Civil and Political Rights.[127]

Application of applicable international law within and linked to armed conflict

Aside from, and in addition to, any determination under *jus ad bellum* of the legality of the use of force in another state, international human rights law will be the primary source of international law determining the legality of the use of drones outside a situation of armed conflict. Within a situation of armed conflict and with respect to acts that represent the requisite nexus, at least non-derogable rights will continue to apply fully, while others may be subject to derogation to the extent 'strictly required by the exigencies of the situation'.[128] Since armed drone strikes are most obviously a threat to life even though they may directly or indirectly affect numerous other human rights, analysis will focus on this 'supreme' right (in the words of the UN Human Rights Committee).[129]

Applicability of human rights law in armed conflicts

In an oft-cited dictum pertaining to the right to life as set out in 1966 Covenant on Civil and Political Rights, the ICJ opined in 1996 that:

> the protection of the International Covenant on Civil and Political Rights does not cease in times of war, except by operation of Article 4 of the Covenant whereby certain provisions may be derogated from in a time of national emergency. Respect for the right to life is not, however, such a provision. In principle, the right not arbitrarily to be deprived of one's life applies also in hostilities. The test of what is an arbitrary deprivation of life, however, then falls to be determined by the applicable *lex specialis*, namely, the law applicable in armed conflict which is designed to regulate the conduct of hostilities.

126 '2010 study on targeted killings', above note 11, paras. 85, 86.
127 N. Lubell, above note 23, pp. 106, 177, 254–255.
128 Human Rights Committee, 'General Comment 29: States of Emergency (Article 4)', UN Doc. CCPR/C/21/Rev.1/Add.11, 31 August 2001.
129 'General Comment No. 6: The right to life (Article 6)', 30 April 1982.

> Thus whether a particular loss of life, through the use of a certain weapon in warfare, is to be considered an arbitrary deprivation of life contrary to Article 6 of the Covenant, can only be decided by reference to the law applicable in armed conflict and not deduced from the terms of the Covenant itself.[130]

Several states argued, unsuccessfully, before the Court that the Covenant – and indeed human rights in general – was not applicable in a situation of armed conflict. This position is rarely heard today, and has been generally discredited.[131]

Relationship between human rights law and international humanitarian law

In contrast, the Court's assertion that whether the right to life has been violated depends on a *renvoi* to the law applicable in armed conflict as *lex specialis*[132] still attracts widespread support. On a superficial reading, this would appear to constitute total deference to IHL. There are, though, a number of reasons for questioning such an assertion. As Christian Tomuschat has noted,[133] the Court's statement was 'somewhat short-sighted'[134] given that in the issue before it, the legality of the threat or use of nuclear weapons, it was unable to 'conclude definitively' based on IHL interpretation whether such threat or use 'would be lawful or unlawful in an extreme circumstance of self-defence'.[135] Second, as he and others have observed, the Court's appraisal of the mutual relationship between IHL and human rights law has been modified in subsequent decisions,[136] notably the Advisory Opinion in the *Wall* case (2004)[137] and the decision in the *Armed*

130 ICJ, *Nuclear Weapons Advisory Opinion*, 8 July 1996, para. 25.

131 Though for the position of Israel and the US, see, e.g., Melzer, above note 11, pp. 79–80. With respect to the American Convention on Human Rights, the Inter-American Commission on Human Rights has specified that 'the contours of the right to life may change in the context of an armed conflict, but . . . the prohibition on arbitrary deprivation of life remains absolute. The Convention clearly establishes that the right to life may not be suspended under any circumstances, including armed conflicts and legitimate states of emergency'. Inter-American Commission on Human Rights, 'Report on Terrorism and Human Rights', Doc. OEA/Ser.L/V/II.116 (doc. 5 rev. 1 corr.), 22 October 2002, para. 86.

132 For a discussion of the application of the principle, see, e.g., Nancie Prud'homme, 'Lex specialis: oversimplifying a more complex and multifaceted relationship?', in *Israel Law Review*, Vol. 40, No. 2, 2007.

133 Christian Tomuschat, 'The right to life – legal and political foundations', in C. Tomuschat, E. Lagrange and S. Oeter (eds), *The Right to Life*, Brill, The Netherlands, 2010, p. 11.

134 Schabas describes it as 'clumsy at best'. See William A. Schabas, 'The right to life', in A. Clapham and P. Gaeta (eds), *Oxford Handbook of International Law in Armed Conflict*, Oxford University Press, forthcoming. Lubell is even harsher on the Court, calling it 'perhaps an inept approach'. N. Lubell, above note 23, p. 240. Milanović calls for *lex specialis* to be 'abandoned as a sort of magical, two-word explanation of the relationship between IHL and IHRL, as it confuses far more than it clarifies'. M. Milanović, 'Norm conflicts, international humanitarian law and human rights law', in Orna Ben-Naftali (ed.), *Human Rights and International Humanitarian Law*, Collected Courses of the Academy of European Law, Vol. XIX/1, Oxford University Press, Oxford, 2010, p. 6.

135 *Ibid*., para. 105.

136 See also in this regard Sir Daniel Bethlehem, 'The relationship between international humanitarian law and international human rights law and the application of international human rights law in armed conflict', unpublished paper, undated but 2012, para. 39.

137 *Ibid.* As set out in para. 106: 'As regards the relationship between international humanitarian law and human rights law, there are thus three possible situations: some rights may be exclusively matters

Activities on the Territory of the Congo case (2005).[138] According to Alston, since both IHL and human rights law apply in the context of armed conflict,

> whether a particular killing is legal is determined by the applicable lex specialis. . . . To the extent that IHL does not provide a rule, or the rule is unclear and its meaning cannot be ascertained from the guidance offered by IHL principles, it is appropriate to draw guidance from human rights law.[139]

Others, including this author, would go even further. Milanović, for example, notes the omission of a reference to IHL as *lex specialis* in the ICJ judgment in the 2005 Congo case, compared with its Advisory Opinions in the *Wall* case and the *Nuclear Weapons* case, and expresses the hope that this was intentional.[140] In a 2011 *European Journal of International Law* blog, he stated:

> A bolder approach to the joint application of IHL and IHRL [international human rights law] would ask whether there are killings which do comply with IHL but are still arbitrary in terms of IHRL. Can, in other words, IHRL during armed conflict impose additional requirements for the lawfulness of a killing to those of IHL? And can these requirements, while more stringent than those of IHL, still be somewhat less stringent than those set out in human rights jurisprudence developed in and for times of normalcy . . .? . . . I think all these questions can be answered with a cautious 'yes'.[141]

Indeed, in its Nuclear Weapons Advisory Opinion, the Court had made it clear that the law applicable in armed conflict (*jus in bello*) was not limited to IHL.[142] Further evidence that it could be overly simplistic to interpret the right to life in a situation of armed conflict merely through the lens of compliance with IHL comes from the meaning of 'arbitrarily deprive'. With respect to the 1966 Covenant on Civil and Political Rights, the term is said to contain 'elements of unlawfulness and injustice, as well as of capriciousness and unreasonableness'.[143]

There is a clear limit to this approach, however. While human rights law has much to bring to the IHL table in terms of limiting violence and promoting

of international humanitarian law; others may be exclusively matters of human rights law; yet others may be matters of both these branches of international law. In order to answer the question put to it, the Court will have to take into consideration both these branches of international law, namely human rights law and, as *lex specialis*, international humanitarian law.'

138 ICJ, *Case Concerning Armed Activities on the Territory of the Congo* (*DRC* v. *Uganda*), Judgment of 19 December 2005, para. 216.

139 '2010 study on targeted killings', above note 11, para. 29.

140 M. Milanović, above note 134, p. 6.

141 M. Milanović, 'When to kill and when to capture?', in *EJIL Talk!*, 6 May 2011, available at: http://www.ejiltalk.org/when-to-kill-and-when-to-capture/.

142 Thus, in para. 42 of its Advisory Opinion, the Court referred to the 'requirements of the law applicable in armed conflict which comprise in particular the principles and rules of humanitarian law'. The law applicable in armed conflict do [sic] indeed comprise *in particular* the principles and rules of humanitarian law, but they are not so limited, comprising elements of international human rights and ('humanitarian') disarmament law. ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion of 8 July 1996, para. 42.

143 Manfred Nowak, *U.N. Covenant on Civil and Political Rights, CCPR Commentary*, N. P. Engel, Kehl, 1993, p. 111. See also N. Melzer, above note 11, p. 93.

humanity (for instance, by contributing to a greater understanding of what constitutes in practical terms 'the principles of humanity' and the 'dictates of public conscience' in the application of the Martens clause), it is not being suggested here that a weapon that is generally lawful under IHL is somehow generally rendered unlawful by human rights law. Lubell, for example, indicates that the laws on the selection of weaponry are rightly addressed by IHL without interference from human rights law.[144] (In fact, it could even be argued that such interference would run the risk of weakening IHL, given that tear gas and expanding bullets, outlawed under IHL as a method and a means of warfare, respectively, might be somehow rendered legitimate as they can be used for law enforcement in compliance with international human rights law.)

Nonetheless, an increased, and increasing, influence of human rights law on the content of *jus in bello*, an area formerly considered the *domaine réservé* of IHL, should be seen not as a threat but as a necessary counterbalance to the more aggressive acts of certain states in response to, what they espouse as, a new legal paradigm in the post-9/11 world.[145] Restraint is not a sign of weakness – it is a sign of strength. With respect to drones, it is said that the CIA refused to deploy the Predator for anything other than surveillance prior to 9/11. The week before the Al Qaeda attacks against the US, the then-Director of the CIA, George Tenet, is reported to have remarked, referring to drones, that it would be 'a terrible mistake' for the 'Director of Central Intelligence to fire a weapon like this'.[146] How prophetic this statement may prove to be.

Conclusion

Drones can enable states to carry out targeted killings efficiently, at relatively little cost, and at minimal risk. In the *Corfu Channel* case,[147] the ICJ stated that:

> the alleged right of intervention as the manifestation of a policy of force, such as has, in the past, given rise to most serious abuses and such as cannot, whatever be the present defects in international organization, find a place in international law. Intervention is perhaps still less admissible in the particular form it would take here; for, from the nature of things, it would be reserved for the most powerful States, and might easily lead to perverting the administration of international justice itself.[148]

144 N. Lubell, above note 23, p. 242.

145 Another way of looking at states' attitude after the 9/11 attacks is to apply IHL rules to situations where human rights applicable to law enforcement operations should be applied.

146 Daniel Benjamin and Steven Simon, *The Age of Sacred Terror*, Random House, New York, 2002, p. 345.

147 The Corfu Channel case resulted from two British Royal Navy ships in the Corfu Strait hitting and detonating sea mines (forty-five British officers and sailors lost their lives and forty-two others were wounded) and subsequent mine clearance operations by the Royal Navy in the Strait, but in Albanian territorial waters. The ICJ held Albania responsible for the explosions and awarded damages to the UK but judged that the clearance operations had violated Albania's sovereignty.

148 ICJ, *Corfu Channel case* (*United Kingdom of Great Britain and Northern Ireland* v. *Albania*), (Merits) Judgment of 9 April 1949, p. 35.

Too often, targeted killings by states, whether using drones or other means, look rather like crossing names off a Mafia hit list. Indeed, as Melzer has observed: 'In the final analysis, . . . measured by the moral standards common to most societies, even targeted killings carried out within the framework of the present legal order often have traits that are more readily associated with criminal behaviour than with acceptable Government policy'.[149] And in the words of a former CIA lawyer: 'The government's power to kill must be carefully controlled – or it could turn into a tyranny worse than terrorism'.[150]

Such control means international legal responsibility for unlawful drone strikes, both at the level of the state and the individual. But who is to be held criminally responsible when civilians are killed either in violation of IHL rules of distinction or proportionality or in violation of fundamental human rights? The operator of the drone? The 'spotters' on the ground (if any)? Those who designate the target as a military objective (who may be paid informants)? The lawyer who authorizes the strike? All of the above? If the strike is unlawful, could it be an example of a joint criminal enterprise under international criminal law, or have one or more of the above aided or abetted an international crime?

Of even greater concern is the prospect of fully autonomous drones making targeting decisions based on a series of programmed vectors, potentially without any human control.[151] Who is then to be held responsible? The manufacturer of the drone? The software programmer? For the moment, there are far more questions than answers.

Moreover, it is only a matter of time before non-state armed groups develop or procure drone technology[152] (or hack into the operation of a state-controlled

149 N. Melzer, above note 11, p. 435.

150 A. J. Radsan, above note 19, p. 8. A study 2011 UK Ministry of Defence study stated that: 'It is essential that, before unmanned systems become ubiquitous (if it is not already too late) that we consider this issue and ensure that, by removing some of the horror, or at least keeping it at a distance, that we do not risk losing our controlling humanity and make war more likely'. *The UK Approach to Unmanned Aircraft Systems*, Development, Concepts and Doctrine Centre, Joint Doctrine Note 2/11, Ministry of Defence, 2011, pp. 5–9. See also Richard Norton-Taylor and Rob Evans, 'The terminators: drone strikes prompt MoD to ponder ethics of killer robots', in *The Guardian*, 17 April 2011, available at: http://www.guardian.co.uk/world/2011/apr/17/terminators-drone-strikes-mod-ethics.

151 According to a 2010 US Air Force report: 'Growth in military use of remotely piloted vehicles has been rapid as forces around the world explore increasingly wider uses for them, including surveillance, strike, electronic warfare, and others. These will include fixed-wing and rotary-wing systems, airships, hybrid aircraft, and other approaches. They will have increasingly autonomous capabilities allowing remote pilots to declare their overall mission intent but permit these systems to adapt autonomously in the local environment to best meet those objectives. . . . Although humans will retain control over strike decisions for the foreseeable future, far greater levels of autonomy will become possible by advanced technologies. These, in turn, can be confidently exploited as appropriate V&V [verification and validation] methods are developed along with technical standards to allow their use in certifying such highly autonomous systems'. US Air Force Chief Scientist, 'Report on technology horizons, a vision for Air Force science & technology during 2010–2030', Doc. AF/ST-TR-10-01-PR, Vol. I, May 2010, pp. 24, 42. See also, Tom Malinowski, Human Rights Watch, 'A dangerous future of killer robots', in *Washington Post*, 22 November 2012, available at: http://www.hrw.org/news/2012/11/22/dangerous-future-killer-robots.

152 In October 2012, the leader of Hezbollah claimed that his group was behind the launch of a drone shot down over Israel by the Israeli Defence Forces on 6 October. Sheikh Hassan Nasrallah asserted that the drone was made in Iran and had flown over 'sensitive sites' in Israel. BBC, 'Hezbollah admits launching drone over Israel', 11 October 2012, available at: http://www.bbc.co.uk/news/world-middle-east-19914441.

drone and assume control).[153] Will not such groups be seeking actively to level the killing field? As a Senior Fellow with the Brookings Institute warned in 2011:

> To believe that drones will remain the exclusive province of responsible nations is to disregard the long history of weapons technology. It is only a matter of time before rogue groups or nations hostile to the United States are able to build or acquire their own drones and to use them to launch attacks on our soil or on our soldiers abroad.[154]

Pandora's box has been opened, but undoubtedly even nastier surprises are yet to emerge.

153 In June 2012, US researchers took control of a flying drone by 'hacking' into its GPS system, acting on a $1,000 (£640) dare from the US Department of Homeland Security (DHS). A University of Texas at Austin team used 'spoofing', a technique where the drone mistakes the signal from hackers for the one sent from GPS satellites. The same method may have been used to bring down a US drone in Iran in 2011. 'Researchers use spoofing to "hack" into a flying drone', in *BBC*, 29 June 2012, available at: http://www.bbc.com/news/technology-18643134.

154 John Villasenor, 'Cyber-physical attacks and drone strikes: the next homeland security threat', *The Brookings Institution*, 5 July 2011, available at: http://www.brookings.edu/papers/2011/0705_drones_villasenor.aspx.

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

Categorization and legality of autonomous and remote weapons systems

Hin-Yan Liu*

Hin-Yan Liu is Max Weber Fellow, European University Institute, and Adjunct Professor, NYU Florence.

Abstract

This article reconsiders the status and legality of both autonomous and remote weapons systems under international humanitarian law. Technologically advanced unmanned military systems are being introduced into the modern battlespace with insufficient recognition of their potential challenge to international humanitarian law. The article questions the understanding of both autonomous and remote weapons systems as 'weapons' and seeks to consider how their use may impact existing legal categories. Their use is then specifically situated to consider the legality of their deployment in certain contexts. Finally, the article raises the question of impunity for the use of both autonomous and remote weapons systems that arise from the inability to attribute responsibility for the harm they cause. It is imperative that law and policy are developed to govern the development and deployment of these advanced weapons systems to forestall these likely situations of impunity.

Keywords: drones, military robotics, robotic soldiers, autonomous weapons systems, automated weapons systems, remote weapons systems, impunity.

* I would like to dedicate this article to the memory of Chelsy Lynn Shillington for her inspiration and encouragement. I am also grateful to the anonymous reviewers for their insightful comments and accept full responsibility for any remaining errors. Email: hin-yan.liu@eui.eu.

doi:10.1017/S1816383113000012X

The technological advances that have enabled the deployment of autonomous and remote weapons systems raise a range of significant legal issues that are exacerbated by the priority of advanced weapons systems in research and funding programmes. The complexity of these legal issues will be compounded by increasing technological sophistication and greater proliferation of advanced weapons systems.

These new technologies of war appear, at first flush, to offer the capacity to reduce incidental injury and collateral damage in armed conflict through their potential to offer a more stringent adherence to the principles of distinction and proportionality. While such ability should be welcomed, what has been surprisingly absent from the legal consideration surrounding their use are the logically anterior questions as to whether both autonomous and remote weapons systems can remain meaningfully categorized as 'weapons', whether the current legal categorization is adequate to regulate their use, and how their use may challenge the existing legal regime.[1] Far from stimulating an exclusively theoretical discussion, posing these questions is fundamental to understanding the nature of these technological advances in situations of armed conflict and other complex violent environments, which is essential for the formulation of appropriate legal regulation.

The emergence of technologically advanced military platforms challenges current notions of what weapons and the 'means and methods of warfare' are because of their capacity to filter and analyse information, to draw conclusions, and to reach decisions. In short, both autonomous and remote weapons systems possess characteristics associated with autonomy. While this is clearest with autonomous weapons systems, which currently influence human decision-making and which may make decisions over the use of lethal force in the near future, contemporary remote weapons systems are capable of acting with varying levels of independence from direct human control that concomitantly decrease the necessity and relevance of human oversight.[2] Indeed, the operational independence of contemporary remote weapons systems can relegate the role of the human supervisor only to suspending or aborting attacks once they have been deployed.

These capacities place such technologically advanced military platforms in a distinctly separate category from all preceding forms of military equipment. Throughout history, from the arrow to the ballistic missile, weapons have been the passive implements and inert tools that human agents have directly manipulated in

1 The terminology and framework are derived from Article 36 of Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, 8 June 1977, 1125 UNTS 3 (entered into force 7 December 1978), Art. 35(1) (hereinafter Additional Protocol I).

2 This article distinguishes only between 'autonomous' and 'remote' weapons systems. This is to differentiate between direct human control over a weapons system, which is retained in remote weapons systems, from the unique departure from direct human control over the use of weapons signalled by introducing autonomy into weapons systems. The ICRC distinguished between different levels of autonomy within weapons systems by formulating three separate categories: remote controlled weapons systems; automated weapons systems; and autonomous weapons systems. ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts', 31st International Conference of the Red Cross and Red Crescent, Geneva: Switzerland, 28 November–1 December 2011, 31IC/11/5.1.2, pp. 38–40.

order to inflict violence, damage, and injury. With the advent of autonomous, and to a lesser extent remote, weapons systems, however, the application of force and ensuing military destructiveness may require minimal, if any, human decision-making or oversight. Autonomous and remote weapons systems appear to subsist between the existing legal categories of 'weapons' and 'combatants'. Classification as mere weapons fails both to acknowledge that these systems do not inflict violence in a direct manner but rather serve as intermediary platforms from which weapons are deployed, and to capture their varying levels of autonomy over the use of force. Conversely, the humanitarian protections afforded to the category of combatant imply the exclusion of machines. This suggests that there are significant conceptual and practical barriers that prevent autonomous and remote weapons systems from being classified as combatants. Regulating autonomous and remote weapons systems simply as weapons will result, at best, in partial, and therefore inadequate, mechanisms that fail to account for the real challenges that they pose.

In this context, the legality of both autonomous and remote weapons systems will be evaluated in light of three current uses and challenges: the targeted killing of 'terrorist' suspects within the context of armed conflict; the civilianization of military force; and their potential to extend cyberwarfare beyond the virtual world into the physical world. These fall within the broader context of the challenges posed by the new technologies of warfare addressed elsewhere in this edition of the *Review*.

Finally, there is the need to address the concomitant questions of responsibility that accompany this autonomous capacity in the deployment of military force. Responsibility in law is a concept that has several disparate dimensions.[3] Thus, although it may be possible for a machine to be responsible in a strictly causal sense for the production of specific results or outcomes,[4] these are not necessarily accompanied by legal or moral responsibility in a role, liability, or capacity understanding of responsibility that usually attaches to human action.[5] This disparity in the capability for legal responsibility between humans and machines leads to serious ramifications concerning the accountability for the use of force that arise from the use of autonomous and remote weapons systems, in turn raising the spectre for allegations of impunity.

This article concludes that international humanitarian law (IHL) in its current manifestation is insufficient to regulate the growing use of autonomous and remote weapons systems. While this is partially due to the permissive nature of IHL in according primacy to military necessity, its failure predominantly arises from its structural inability to cope with the challenges raised by this novel means and method of armed conflict. That the source of the problem is rooted in the question

3 H. L. A. Hart and John Gardner, *Punishment and Responsibility: Essays in the Philosophy of Law*, Oxford University Press, New York, 2008, pp. 211–237.

4 *Ibid*., p. 214.

5 *Ibid*., pp. 211–237. Role responsibility considerations may be relevant to autonomous and remote weapons systems because of the likelihood that their efficacy will be assessed upon fulfilment of their objectives. This, however, will fall foul of the disjuncture created between role and outcome responsibility, ultimately exacerbating the diffusion of responsibility for the consequences of utilizing such weapons systems.

of categorization, however, is simultaneously its source of hope. This is because the current system of IHL is capable of accommodating autonomous and remote weapons systems provided that a method for their categorization in law is negotiated, accepted, and legitimated, and provided that a system for allocating and attributing responsibility for their use can be agreed upon. At this watershed in the development and deployment of autonomous and remote weapons systems, it is particularly timely to undertake a rigorous critical consideration of these issues. Addressing these issues now would contribute to avert similar allegations of impunity that have plagued the modern private military company industry due to the questions regarding their legal categorization and the mechanisms of accountability.[6]

This article begins by sketching out the contemporary state of development for autonomous and remote weapons systems and by providing some historical context. The article then moves to outline the pressures that will push for greater automation of these advanced weapons systems that will result in their increasing deployment in the near future. Then, for the purposes of reviewing their legality, the article critically analyses whether autonomous and remote weapons systems can be appropriately classified as weapons or, more broadly, as means or methods of warfare. In this vein, the article continues by illustrating various issues that arise from applying current weapons laws to autonomous and remote weapons systems. The legality of remote weapons systems will then be tentatively situated within the context of their current use in the targeted killing campaigns of 'terrorist' suspects, and within the context of some legal implications that may arise with the greater proliferation of both autonomous and remote weapons systems in the near future. Finally, the article will address the claim that advanced weapons systems may become superior to human agents in the battlespace in their adherence to humanitarian principles, while highlighting the persistent responsibility gap with respect to autonomous and remote weapons systems and the potential for impunity they will create. This article concludes that IHL in its current manifestation is insufficient to regulate the growing use of autonomous and remote weapons systems.

The current state of autonomous and remote weapons systems

Due to the secrecy shrouding military technology, it is difficult to ascertain precisely the current cutting-edge capability of military robotics. Furthermore, even if it were possible to capture their contemporary capacity, the rapidity with which these technologies develop would quickly render this picture obsolete.[7] For the purposes

6 See Hin-Yan Liu, 'Leashing the corporate dogs of war: the legal implications of the modern private military company', in *Journal of Conflict and Security Law*, Vol. 15, 2010, pp. 141–168; and Hin-Yan Liu, *Law's Impunity: Responsibility and the Modern Private Military Company*, Hart, Oxford, 2014 (forthcoming).

7 Peter W. Singer, *Wired for War*, Penguin, New York, 2009, pp. 94–108.

of this article, it will only be necessary to provide a brief factual sketch, which can be formed from the numerous examples of autonomous and remote weapons systems that are, or have recently been, deployed in the battlespace. For example, Ronald Arkin describes a range of weaponized unmanned military vehicles produced by a number of different companies that are currently available for service on land, sea, and air.[8] On land, available weaponized systems range from the Samsung Techwin SGR-A1 intelligent surveillance and security guard robot, which is equipped to deliver lethal or non-lethal force either with or without human decision-making, to the iRobot Packbot and TALON SWORDS platforms that are not autonomous.[9] In the air, the most well-known weaponized unmanned aerial vehicles (UAVs) are the MQ-1 Predator and the MQ-9 Reaper of the US Air Force.[10] These have gained notoriety for their role in the targeted killings of suspected 'terrorists' and were reported to be responsible for over seven hundred deaths in the eighteen month period from the beginning of the Obama Administration to the end of June 2010 in Pakistan alone.[11] Furthermore, P. W. Singer adds that outer space may soon be a potential zone of conflict opened up to robotic warfare.[12] The combined picture is one where unmanned military vehicles are fulfilling the full range of military roles and are fast becoming ubiquitous in the battlespace.

To date, these weapons systems have been more remote than autonomous: they are teleoperated by humans rather than being capable of autonomous operation. Teleoperated weapons systems have a long lineage that pre-dates the First World War,[13] and are relatively uncontroversial from the perspective of IHL because they are ultimately under the full control of human operators.[14] In other words, remote weapons systems, in the strict sense, are unlikely to engage any additional dimension of IHL in relation to other conventional weapons systems. Instead, it is the rising levels of autonomy that categorically differentiate

8 Ronald Arkin, *Governing Lethal Behaviour in Autonomous Robots*, Chapman & Hall/CRC, Boca Raton, 2009, pp. 7–27.

9 *Ibid*., pp. 10–14. See also, Armin Krishnan, *Killer Robots*, Ashgate, Farnham, 2009, pp. 28–30.

10 A. Krishnan, above note 9, pp. 27–28.

11 BBC News, 'Mapping US drone and Islamic militant attacks in Pakistan', in *BBC News*, 22 July 2010, available at: http://www.bbc.co.uk/news/world-south-asia-10648909 (last visited 9 December 2012). See also The Bureau of Investigative Journalism, 'Covert war on terror – the data', in *The Bureau of Investigative Journalism*, 8 May 2012, available at: http://www.thebureauinvestigates.com/category/projects/drone-data/ (last visited 9 December 2012), and the section entitled 'Targeted killings and remote weapons systems' below.

12 P. W. Singer, above note 7, pp. 120–122. In this context, it should be noted that while nuclear and other weapons of mass destruction are prohibited in orbit or on celestial bodies, conventional military activities are only forbidden on celestial bodies per Article 4 of the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, UNGA Res. 2222 (1966). This leaves open the potential for lawful conventional military activity to take place in orbit under the Treaty.

13 For a brief history, see P. W. Singer, above note 7, pp. 46–65, and A. Krishnan, above note 9, pp. 13–32.

14 Full and direct, albeit remote, human control should ground concomitant responsibility for the use of these weapons systems. The most uncontroversial category of unmanned vehicle would be those that 'are used for any purpose other than the delivery of kinetic force against enemy personnel and objects', see William Boothby, *Weapons and the Law of Armed Conflict*, Oxford University Press, Oxford, 2009, pp. 229–230.

autonomous from remote weapons systems and their predecessors. In the United States, this process took place in the 1980s to offset the Soviet threat with conventional weapons systems.[15] Despite the subsequent lull in the pace of development arising from the 1990s peace dividend, interest in advanced weapons systems was soon reignited with the maturation of these military technologies combined with a growing appreciation of the range of roles that they may play in future armed conflict and other complex environments. As a result, research, development, and deployment have surged in the new millennium as these advanced military systems are proving their utility and tentative steps towards weapons autonomy are being made.[16]

In contradistinction to the relatively long history of remote weaponry, the technological developments that have enabled the possibility of increasingly autonomous weapons systems have taken place only recently. Rather than simply constituting a small step in the same direction, the introduction of autonomy into weaponized systems, however, poses many unique challenges to IHL. This is because the hitherto human monopoly over the decision to deploy or inflict violence is challenged by autonomous weapons systems. Furthermore, the capacity for autonomous decision-making may elevate advanced weapons systems from the category of passive military materiel towards that of the active combatant. It should be emphasized at this point that it is not the independent capacity to kill or maim that is the objection being raised here,[17] but rather that the weapons system itself is able to *decide*, or significantly influence the decision, whether or not to inflict violence. This decision-making capacity is, however, accompanied by neither the prospect of responsibility nor accountability, thereby eroding the incentives to comply with the rules on the conduct of hostilities. This questions the adequacy of IHL in its current state because its categories have not yet been adapted to accommodate non-human decision-making entities capable of inflicting violence. These advanced weapons system developments also raise challenges under international criminal law insofar as the allocation and attribution of responsibility for unlawful harm is concerned.[18] The difficulty of categorizing autonomous weapons systems in particular is evident in the terminological confusion that plagues this topic, and is reinforced in attempts to apply the current state of law to the category of weapons systems addressed below. It is, however, important first to briefly illustrate some of the pressures that drive the trend towards autonomy in order to show that this is unlikely to be a temporary phenomenon.

15 A. Krishnan, above note 9, pp. 23–24.

16 *Ibid*., pp. 33–59. See also, Human Rights Watch and International Human Rights Clinic (Harvard Law School), *Losing Humanity: The Case Against Killer Robots*, November 2012, pp. 6–20.

17 The independent capability of weapons to inflict violence is apparent in mines for instance, and is usually objected to on the grounds of indiscriminateness or existence of threat after the cessation of hostilities.

18 It is clear, for example, that the Rome Statute for the International Criminal Court only contemplates the inclusion of natural persons as perpetrators of the international crimes it establishes. See Article 25(1): 'The Court shall have jurisdiction over *natural persons* pursuant to this Statute' (emphasis added). While this has been interpreted to exclude legal persons such as corporations, the emergence of autonomous weapons systems challenges both the presumption that only natural persons can be perpetrators, and also the continued tenability of the provision of Article 25(1).

INTERNATIONAL REVIEW of the Red Cross

Trajectories for future development

In 2001 the United States (US) Congress mandated specific developmental goals for significant proportions of combat vehicles to be unmanned in the near future.[19] Later, in 2007, Congress stipulated a strong policy preference for unmanned systems in Department of Defense acquisition programmes by reversing the onus of proof: the development of manned programmes now requires justification through a certification scheme that unmanned systems would be incapable of fulfilling system requirements.[20] The Department of Defense subsequently (in 2007) devised a coordinated plan to develop and deploy an increasingly sophisticated array of unmanned systems over the next twenty-five years.[21] These policy incentives complement military utility, which together provide a clear practical driving force behind the desire to field autonomous weaponry: not only are advanced weapons systems cheaper to produce, operate and maintain, but they are perceived to be more capable and efficient than their low-tech, directly human-operated counterparts.[22] Furthermore, it has been claimed that both autonomous and remote weapons systems enable an increase in the projection of state power despite declining military recruitment figures and, in decreasing the exposure of friendly forces to danger, will significantly lower the number of casualties and remove the democratic resistance to military deployment.[23]

There are clear pressures towards automation. Armin Krishnan points, for instance, to the force multiplier effect gleaned from automating even basic processes within remote systems, whereby one person will be capable of controlling several remote weapons systems.[24] This push towards automation is reinforced by the perceived performance superiority of such systems that may be capable of enhancing the abilities of human combatants. Ronald Arkin has suggested that advanced systems may be able to analyse and collate large amounts of information thereby enabling a speedier and better informed reaction, and has further pointed out that autonomous systems maybe capable 'of independently and objectively monitoring ethical behaviour in the battlefield by all parties and reporting infractions that might be observed'.[25] These perceived benefits may be enhanced

19 Section 220 of the National Defense Authorization Act for Fiscal Year 2001 (Public Law 106–398; 114 Stat. 1654A–38): '(a) GOAL. – It shall be a goal of the Armed Forces to achieve the fielding of unmanned, remotely controlled technology such that – (1) by 2010, one-third of the aircraft in the operational deep strike force aircraft fleet are unmanned; and (2) by 2015, one-third of the operational ground combat vehicles are unmanned'.

20 Section 941(b)(2) of National Defense Authorization Act for Fiscal Year 2007 (Public Law 109-364; 120 Stat. 2083).

21 US Department of Defense, 'Unmanned systems roadmap 2007–2032', Washington DC, 2007, available at: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA475002 (last visited 18 January 2012).

22 Michael Schmitt, 'War, technology and the law of armed conflict', in Antony Helm (ed.), *War in the 21st Century: Weaponry and the Use of Force*, Naval War College Studies: International Law Studies, Vol. 82, 2006, p. 149.

23 Hyder Gulam and Simon Lee, 'Uninhabited combat aerial vehicles and the law of armed conflict', in *Australian Army Journal*, Vol. 3, No. 2, 2006, p. 126.

24 A. Krishnan, above note 9, pp. 35–37.

25 R. Arkin, above note 8.

by the reduction of military budgets in many Western states.[26] Militaries may scramble towards advanced technological systems to compensate for lost capabilities.

Finally, although this does not directly affect considerations of legality, it should be noted that the development of both autonomous and remote weapons systems is not unique to the traditional militarily advanced states such as the United States, or even Western NATO countries more broadly.[27] For instance, Iran has recently unveiled its first unmanned bomber, and China has also showcased a new fleet of drones that raise questions of broader strategic significance.[28] This revolution in military technology not only upsets the current balance of military capabilities, but may also have subtler legal effects. This is because the lack, or inadequacy, of legal regulation over both autonomous and remote weapons systems would be more difficult to rectify once these technologies have proliferated.

Terminological hurdles: weapon, means or method of warfare

While the terminology applied to this topic has thus far been used consistently, it is important now to elaborate upon these terms and the applicable legal definitions. This will illustrate that IHL, as currently conceived, is incapable of coherently categorizing both autonomous and remote weapons systems.

It must be noted at the outset that the terms 'weapon, means or method of warfare'[29] have not been exhaustively defined in IHL or applicable legal instruments. In lieu of a legal definition, reliance is placed instead on the constellation of stable and identifiable characteristics that shape these terms. This is evident in the plain linguistic meaning of 'weapon'; the dictionary definition for which is primarily 'a thing designed or used for inflicting bodily harm or physical damage' and secondarily as 'a means of gaining an advantage or defending oneself in a conflict or contest'.[30] Thus, the conflation between the physical implements through which violence is inflicted, and the techniques by which it is used for these purposes, share early etymological roots that imply a fundamental connection. Indeed it would be nonsensical to consider the characteristics of a weapon isolated from the context of

26 See for instance, Nick Hopkins, 'MoD announces further 4,200 armed forces personnel cuts', in *The Guardian*, 18 January 2012, available at: http://www.guardian.co.uk/politics/2012/jan/17/mod-4200-armed-forces-cuts?INTCMP=SRCH (last visited 18 January 2012).

27 At least twenty countries are known to possess significant military robotics research programmes. See A. Krishnan, above note 9, p. 13.

28 BBC News, 'Iran unveils first bomber drone', in *BBC News*, 22 August 2010, available at: http://www.bbc.co.uk/news/world-middle-east-11052023 (last visited 9 December 2012); and Robert Beckhusen, 'China unveils its new drone fleet to the world', in *Wired*, 28 November 2012, available at: http://www.wired.co.uk/news/archive/2012-11/28/china-unveils-new-drones (last visited 9 December 2012). For a glimpse into how the US could lose the robotic revolution, and for the growing non-state use of military robotics, see P. W. Singer, above note 7, pp. 237–278.

29 Additional Protocol I of 1977, Art. 36.

30 *Oxford Dictionary of English*, Oxford University Press, Oxford, 2005.

its use, which is reflected in the ICRC Guide to the Legal Review of New Weapons, Means and Methods of Warfare.[31]

That the understanding of what a 'weapon' is has been assumed to be commonly held may be inferred from the fact that this term has not been defined in the conventions and provisions that are directly relevant.[32] Yet, commentators have alluded to the meaning of 'weapons' under international law. William Boothby suggests that weapons are 'tools of warfare, of killing, maiming, and destruction',[33] while Justin McClelland suggests that the term 'connotes an offensive capability that can be applied to a military object or enemy combatant'.[34] According to the ICRC Guide, the 'terms "means and methods of warfare" designate the tools of war and the ways in which they are used'.[35] The Guide refers to national military documents to further illuminate the term, with those from Australia and the United States in particular providing definitions that are not self-referential. The Australian Instruction provides that a 'weapon' is 'an offensive or defensive instrument of combat used to destroy, injure, defeat or threaten. It includes weapon systems, munitions, sub-munitions, ammunition, targeting devices, and other damaging or injuring mechanisms'.[36] The US Department of Defense's Law of War Working Group differentiates between the terms 'weapon' and 'weapon system'. The former refers to 'all arms, munitions, materiel, instruments, mechanisms, or devices that have an intended effect of injuring, damaging, destroying or disabling personnel or property' while the latter is more broadly conceived to include 'the weapon itself *and those components required for its operation, including new, advanced or emerging technologies*'.[37] The present article adopts this distinction between a weapon and a weapons system. This is because autonomous and remote weapons systems cannot be narrowly categorized as only weapons because they do not inflict damage or harm in a direct manner, as a mine or a cruise missile would. Instead, they are appropriately categorized as a weapons system because they serve as an intermediary platform from which the actual weapons are deployed. Finally,

31 For example, it is not the inherent characteristics of a weapon that are of concern under international law, but rather the manner in which it is used: 'The aim of Article 36 [of Additional Protocol I] is to prevent the *use* of weapons that would violate international law in all circumstances and to impose restrictions on the *use* of weapons that would violate international law in some circumstances' (emphasis added). International Committee of the Red Cross Geneva, 'A guide to the legal review of new weapons, means and methods of warfare: measures to implement Article 36 of Additional Protocol I of 1977', in *International Review of the Red Cross*, Vol. 88, No. 864, 2006, p. 933.

32 Indeed, even in the Commentaries for Article 36, Jean de Preux makes numerous references to the term 'weapon' without elaborating upon its characteristics or attempting to provide a definition. Claude Pilloud *et al.*, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, ICRC and Kluwer, 1987, paras. 1463–1482. The same holds true for The Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects as amended on 21 December 2001.

33 W. Boothby, above note 14, p. 1.

34 Justin McClelland, 'The review of weapons in accordance with Article 36 of Additional Protocol I', in *International Review of the Red Cross*, Vol. 85, No. 850, 2003, p. 404. This connotation is especially noteworthy because a weapon could not, by this definition, be used to target civilians. Clearly, this approach would need to be broadened to account for other uses of weapons.

35 ICRC, above note 31, p. 932, fn 1.

36 *Ibid.*, p. 937, fn 17.

37 *Ibid.*, p. 937, fn 17 (emphasis added).

the US Law of War Working Group's definition is limited to the military systems that are integrally associated with the use of force; this has the merit of appropriately excluding non-violent support systems, such as surveillance platforms, from the purview of a weapons system.

Turning next to means and methods of warfare, it is clear that these terms are conflated with the weapon itself, at least insofar as the review of the legality under Article 36 of Additional Protocol I is concerned. Kathleen Lawand writes: 'A new weapon – that is, a proposed *means* of warfare, cannot be examined in isolation from the way in which it is to be used – that is, without also taking into account the *method* of warfare associated with it'.[38] The interconnectedness of these terms arises from the expansive nature of Article 36, which does not clearly distinguish between 'weapons' and 'means of warfare'; in other words, Article 36 may be tautological in order to cast as broad net as possible. The 'method' of warfare, on the other hand, 'is usually understood to mean the way in which weapons are used'.[39] Justin McClelland usefully suggests that the terms 'means' and 'methods' should be read together in order to 'include those items of equipment which, whilst they do not constitute a weapon as such, nonetheless have a direct impact on the offensive capability of the force to which they belong'.[40] While the example he gives is a mine clearance vehicle, when read together the terms means and methods should be extended to autonomous and remote weapons systems in order to ground rigorous legal review. This is because advanced weapons systems may deploy existing conventional weapons in novel ways that might otherwise circumvent a holistic approach to the review of legality, as discussed below. This is clearly a useful approach with which to address autonomous and remote weapons systems because in 'military technological thinking and research, atomistic ontologies are being replaced by thinking in terms of systems, networks, and swarms'.[41] In other words, adhering to strict divisions between armed and unarmed systems or between autonomous and remote systems may become untenable due to the close interconnectedness of these systems.

Leaving aside the terminological questions that hang over 'weapon, means and method of warfare', the capacity for autonomous decision-making pushes these technologically advanced systems to the boundary of the notion of 'combatant'. Confusion between these categories is evident in the range of approaches by commentators in a recent special issue of *Philosophy and Technology*. For example, Ugo Pagallo uses the term 'robot soldier'[42] in a clear departure from the

38 Kathleen Lawand, 'Reviewing the legality of new weapons, means and methods of warfare', in *International Review of the Red Cross*, Vol. 88, No. 864, 2006, p. 927.

39 Isabelle Daoust, Robin Coupland and Rikke Ishoey, 'New wars, new weapons? The obligation of states to assess the legality of means and methods of warfare', in *International Review of the Red Cross*, Vol. 84, No. 846, 2002, p. 352.

40 J. McClelland, above note 34, p. 405.

41 Mark Coeckelbergh, 'From killer machines to doctrines and swarms, or why ethics of military robotics is not (necessarily) about robots', in *Philosophy and Technology*, Vol. 24, 2011, p. 273.

42 Ugo Pagallo, 'Robots of just war: a legal perspective', in *Philosophy and Technology*, Vol. 24, 2011, pp. 307–323. See also, Kenneth Anderson and Matthew Waxman, 'Law and ethics for robot soldiers', in *Policy Review*, No. 126, 2012.

established categories of IHL, although clearly alluding to the potential for autonomous weapons systems to mirror the capability of combatants, while other authors in that special issue consider these as only weapons.[43] The German military manual, which provides that 'combatants are persons who may take a direct part in hostilities, i.e., participate in the use of a weapon or a weapon-system in an indispensable function', indicates potential for the confusion between means and methods of warfare and combatants.[44] Although this characterization was used in the context of differentiating categories of non-combatants who are members of the armed forces, the circularity of this definition illustrates precisely the difficulties associated with defining 'weapon' and 'weapons system'. The point is, however, that aside from the explicit reference to 'persons', the definition of a combatant as an operator of a weapon or a weapon system illustrates the potential for classifying an autonomous weapons system as a combatant, at least in theoretical terms.

This article will not seek to consider autonomous weapons systems as combatants because of the profound implications this would entail for IHL. Rather, the point is to highlight the potential ontological impact of autonomy on weapons systems, questioning their categorization as strictly 'weapons'. The use of autonomous and remote weapons systems that possess autonomous capacities clearly poses challenges to contemporary IHL.

Applying current weapons laws to autonomous and remote weapons systems

While the previous section tackled the terminological questions associated with the categorization of autonomous and remote weapons systems, this section analyses their compliance with currently applicable laws governing weaponry.[45] It should be noted at the outset that there is currently neither explicit prohibition of autonomous and remote weapons systems nor any international regulation for their deployment in situations of armed conflict per se. There was the potential for unmanned combat aerial vehicles (UCAVs) to breach specific Treaty-based restrictions because they share some characteristics both with cruise missiles and with bombers. For example, ground launched cruise missiles within certain mass parameters were prohibited

43 Linda Johannson, 'Is it morally right to use unmanned aerial vehicles (UAVs) in war?', in *Philosophy and Technology*, Vol. 24, 2011, pp. 279–291; and Marcus Schulzke, 'Robots as weapons in just wars', in *Philosophy and Technology*, Vol. 24, 2011, pp. 293–306.

44 Military Manual of Germany, as quoted in Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law, Volume I: Rules,* ICRC and Cambridge University Press, Cambridge, 2005, p. 13 (hereinafter 'ICRC Study').

45 The question of categorizing autonomous weapons systems as combatants is not considered further in this article. It should also be noted that the right of the belligerents to choose their means and methods of warfare is not unlimited, see ICRC, above note 31, p. 931. See also, Article 22 of the 1907 Hague Regulations Respecting the Laws and Customs of War on Land, and Additional Protocol I, Article 35(1), above note 1.

under the Intermediate-Range Nuclear Forces Treaty 1987.[46] UCAVs, however, could be distinguished from cruise missiles because they were designed to return to base and because they possessed flight control capable of altering the route to the target. Similarly, UCAVs could be excluded as a bomber under the Strategic Arms Reduction Treaty (START)[47] because of differences in both range and payload. These distinctions led the US authorities to consider that UCAVs did not generally violate these specific Treaty obligations.[48]

Legal review of new weapons, means, and methods of warfare

As alluded to above, however, the lack of directly applicable regulation does not absolve legal considerations surrounding the intrinsic characteristics of the weapons themselves, or their use in 'some or all circumstances', because all new means and methods of warfare must be subjected to legal review. Although this requirement is most recently expressed in Article 36 of Additional Protocol I of 1977 to the Geneva Conventions, its roots may be traced back to the 1868 St Petersburg Declaration that is regarded as the first major international instrument to prohibit the use of a specific weapon in armed conflict.[49] That 'the use of means and methods of warfare' may be subject to legal consideration is considered to be customary IHL.[50] These criteria were elaborated upon by the International Court of Justice in its 1996 Advisory Opinion:

> The cardinal principles contained in the texts constituting the fabric of humanitarian law are the following. The first is aimed at the protection of the civilian population and civilian objects and establishes the distinction between combatants and non-combatants; States must never make civilians the object of attack and must consequently never use weapons that are incapable of distinguishing between civilian and military targets. According to the second principle, it is prohibited to cause unnecessary suffering to combatants: it is accordingly prohibited to use weapons causing them such harm or uselessly

46 USs Department of State, 'Treaty between the United States of America and the Union of the Soviet Socialist Republics on the Elimination of Their Intermediate-Range and Shorter-Range Missiles', 1988, available at: http://www.state.gov/www/global/arms/treaties/inf2.html (last visited 9 December 2012).

47 US Department of State, 'Definitions Annex: Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Reduction and Limitation of Strategic Offensive Arms', 1991, available at: http://www.state.gov/www/global/arms/starthtm/start/defini.html#36 (last visited 9 December 2012).

48 The US did, however, abandon the deployment of the Harpy, an Israeli UCAV for fear of violating the 1987 Treaty. See H. Gulam and S. Lee, above note 23, p. 130; and Antony Lazarski, 'Legal implications of the uninhabited combat aerial vehicle, in *Air & Space Power Journal*, 2001, available at: http://www.airpower.maxwell.af.mil/airchronicles/cc/lazarski.html (last visited 9 December 2012).

49 Adam Roberts, and Richard Guelff, *Documents on the Laws of War*, Oxford University Press, Oxford, 2000, p. 53.

50 J.-M. Henckaerts and L. Doswald-Beck, above note 44, Rules 70 to 86, pp. 237–296. For an opposing perspective, see David Turns, 'Weapons in the ICRC Study on Customary International Humanitarian Law', in *Journal of Conflict and Security Law*, Vol. 11, 2006, pp. 201–237.

> aggravating their suffering. In application of that second principle, States do not have unlimited freedom of choice of means in the weapons they use.[51]

Since Article 36 of Additional Protocol I is considered to embody the customary law obligation of reviewing weapons, it forms a useful starting point. While the text of the Article itself does not elaborate upon the scope or meaning of the phrase, the Commentary to the Article provides that:

> The words 'methods and means' include weapons in the widest sense, as well as the way in which they are used. The use that is made of a weapon can be unlawful in itself, or it can be unlawful only under certain conditions . . . However, a weapon that can be used with precision can also be abusively used against the civilian population. In this case, it is not the weapon which is prohibited, but the method or the way in which it is used.[52]

Similarly, the ICRC Guide provides that 'the legality of a weapon does not depend solely on its design or intended purpose, but also on the manner in which it is expected to be used on the battlefield'.[53] These sources suggest that a weapon which is prima facie lawful, or which has previously passed legal review, may subsequently be used in a manner that is deemed unlawful. This raises significant implications for the legal review of both autonomous and remote weapons systems. These advanced weapons systems cannot strictly be categorized as weapons because they generally serve as an intermediary platform from which existing weapons, which have previously passed legal review, are deployed. Yet, the way these conventional weapons are used has been drastically altered when deployed by autonomous or remote weapons systems; consequently, a new legal review should be required that takes into account these new means and methods of warfare from a holistic perspective.

William Boothby has provided an initial analysis of the legality of autonomous and remote weapons systems.[54] His primary characterization, however, concerns the ability of an unmanned system to deploy or control weapons. Although there is a requirement under Article 36 of Additional Protocol I to review the legality of systems that do not control weapons, he considers it is unlikely that these systems will contravene any of the relevant considerations.[55] Moving on to what he terms 'unmanned combat vehicles', he draws attention to relevant legality considerations. Where the prior decision concerning an attack remains with a person, he sees no relevant issues being raised.[56] It is the autonomous decision-making with relation to an attack that 'must be considered by the weapons reviewer in the light of the precautions which are required by international law before an attack is launched'.[57]

51 International Court of Justice (ICJ), *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, ICJ Reports, 1996, para. 78.
52 Jean de Preux, in C. Pilloud *et al.*, above note 32, para. 1402.
53 ICRC, above note 31, p. 938.
54 A cursory analysis is provided in W. Boothby, above note 14, pp. 229–232.
55 *Ibid.*, pp. 229–230.
56 *Ibid.*, p. 230.
57 *Ibid.*, p. 230.

In such instances, the legal reviewer must consider the ability of the system to adhere to the discrimination requirement to distinguish between civilians and combatants. He emphasizes that:

> human decisions, some of them taken in advance of the UCV [unmanned combat vehicle] mission, can suitably constrain the timing, location, objective, and means of any UCV attack, the algorithms, depending on their sophistication and reliability, may be able effectively to restrict attacks to objects recognized by the software as legitimate military objectives.[58]

While William Boothby may be strictly correct with relation to determinations of legality under IHL, he does not go on to consider the question of responsibility for the actions of a remote weapons system.

Finally, Noel Sharkey has drawn attention to the slippery slope engendered by the atomized nature of weapons review, especially in the area of autonomous and remote weapons systems:

> Take the case of the MQ1-Predator UCAV. JAG [Judge Advocate General's Corps] first passed it for surveillance missions. Then when it was armed with Hellfire missiles, JAG said that because it had previously passed both the Predator and the Hellfire missiles, their combination did not require a review . . . If arming robots keeps soldiers out of risk and the weapons are already legal, then there might be no legal opposition to deploying robots with weapons.[59]

While this type of reasoning may be appropriate for the legal review of other combinations of weapons and weapons systems, applying such an approach to both autonomous and remote weapons systems fails to recognize the potential for radical transformation in the conduct of armed hostilities raised in this specific context.[60]

At a minimum, new means and methods of warfare must satisfy the two principles of unnecessary and superfluous injury,[61] and distinction.[62]

Superfluous injury or unnecessary suffering

The prohibition of means and methods of warfare that are of a nature to cause superfluous injury or unnecessary suffering under IHL is found in Rule 70 of the ICRC Study.[63] William Boothby considers this issue irrelevant in the present context because the legality of the weaponry that autonomous and remote

58 *Ibid*., p. 233.
59 Noel Sharkey, 'Cassandra or false prophet of doom: AI robots and war', in *IEEE Intelligent Systems*, Vol. 23, 2008, p. 17.
60 On these facts, because the Predator is strictly a remote weapons system, combining the review may not be problematic since it may not significantly alter the means and methods of warfare that previously passed the legal review test. By contrast, autonomous weapons systems may significantly alter the legality review.
61 W. Boothby, above note 14, pp. 55–68.
62 *Ibid*., pp. 69–85. See also ICJ, above note 51, p. 257.
63 J.-M. Henckaerts and L. Doswald-Beck, above note 44, pp. 237–244.

weapons systems deploy is independently reviewed.[64] Where the weapons system itself does not inflict superfluous injury or unnecessary suffering, this is certainly correct. While there may be some exceptions, such as where an autonomous or remote weapons system is itself the weapon (such as the US military's Switchblade),[65] it is indeed unlikely that remote and autonomous weapons systems will challenge this principle.

Discrimination

The customary IHL basis for the principle of discrimination is encapsulated in Rules 11 and 12 and supported by Rule 71, which prohibits the use of weapons that are by nature indiscriminate.[66] With regard to current technological capabilities, roboticist Noel Sharkey writes that 'no autonomous robots or artificial intelligence systems have the necessary skills to discriminate between combatants and innocents'.[67] The poor record of autonomous and remote weapons systems in distinguishing threats was poignantly illustrated by the shooting down of the civilian Iran Air Flight 655 by *USS Vincennes* in July 1988 resulting in the deaths of all 290 on board.[68] The warship was equipped with an automated Aegis system which marked the civilian passenger jet as an 'assumed enemy' prior to the crew authorizing weapon launch.[69] During the course of the 2003 invasion of Iraq, an almost identical scenario resulted in the downing of two allied planes when US Patriot missile batteries classified the aircraft as Iraqi rockets.[70] Thus, there is a strong case against the capacity of an autonomous and remote weapons system to fulfil the discrimination requirement, even in instances where humans ultimately make the final decision to strike.[71]

Precautionary requirements

The principle of discrimination is further supported by the distinct requirement embodied within Rule 17 that requires that parties to the hostilities take

64 W. Boothby, above note 14, p. 230.

65 See Spencer Ackerman, 'US Troops will soon get tiny kamikaze drone', in *Wired Magazine*, 18 October 2011, available at: http://www.wired.com/dangerroom/2011/10/tiny-kamikaze-drone/ (last visited 18 January 2012).

66 J.-M. Henckaerts and L. Doswald-Beck, above note 44, pp. 244–250.

67 Noel Sharkey, 'Grounds for discrimination: autonomous robot weapons', in *RUSI Defence Systems*, Vol. 11, 2008, p. 87.

68 P. W. Singer, above note 7, pp. 124–125.

69 *Ibid.*, p. 125.

70 *Ibid.*, p. 125. While this concerns 'blue-on-blue' fire and thus does not engage discrimination in the sense of being able to differentiate between combatants and civilians, it does illustrate the crudity of current systems in this area.

71 Seen in this light, it may be aberrant that a body of jurisprudence has, however, emerged in the United States attesting to the superiority of robotic judgement and requiring deference to this judgement by human beings. In *Klein v. US.* (13 Av.Cas. 18137 [D. Md. 1975]), the court found that in cases of negligence, and whilst the pilot is not required to use the autopilot on a landing, his failure to use it may be inconsistent with good operating procedure and may be evidence of a failure of due care. In *Wells v. U.S.* (16 Av.Cas. 17914 [W.D. Wash. 1981]), another court inferred negligence on the part of the human pilot from evidence that he switched from automatic pilot to manual control in a crisis situation.

precautions in the choice of means and methods of warfare in order to avoid or minimize incidental injury to civilians and collateral damage to civilian objects.[72] As indicated by William Boothby, precaution is likely to be the most relevant ground for considering the legality of autonomous weapons systems. This will require human involvement in the decision-making process either 'in the loop' or by constraining 'the timing, location, objective, and means' of an attack such that the weapons system would be capable of restricting attacks only to legitimate military targets.[73] These are, however, two very different situations: in the former, there is continuous human monitoring in contradistinction to the latter where human decision-making is only involved during the initial stages of an attack. This difference becomes important in the context of Rule 19:[74] in the latter situation, as Boothby acknowledges, it is likely that human decision-making will be required unless the initial set of constrains remain valid throughout the entire operation.[75]

The principle of proportionality

A further consideration concerns the principle of proportionality. While some commentators seek to analyse proportionality in the context of weapons causing superfluous injury or unnecessary suffering, Yoram Dinstein, among many others, criticizes such an approach because proportionality is a principle that arises with the consideration of incidental injury to civilians and collateral damage to civilian objects in relation to the military objective pursued.[76] Thus, the question of proportionality may arise independent of discrimination considerations. Although the term proportionality may not be specifically mentioned in Additional Protocol I, it does find expression in Article 51(5)(b) which prohibits expected incidental injury and collateral damage to civilians or civilian objects excessive in relation to the military objective anticipated. This obligation is reiterated in Article 57(2)(a)(iii) of Additional Protocol I and Article 8(2)(b)(iv) of the Rome Statute which establishes such 'clearly excessive' loss of life, injury, or damage as a war crime. Thus, proportionality is an important consideration where there is potential for unjustifiable effects for civilians.

With regard to autonomous and remote weapons systems in relation to this criterion, Noel Sharkey writes: 'there is no sensing or computational capability

72 J.-M. Henckaerts and L. Doswald-Beck, above note 44, pp. 56–58. This Rule is further supplemented by Rules 18–21, *ibid*., pp. 58–67.

73 W. Boothby, above note 14, p. 233.

74 'Each party to the conflict must do everything feasible to cancel or suspend an attack if it becomes apparent that the target is not a military objective or that the attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated'. See J.-M. Henckaerts and L. Doswald-Beck, above note 44, Rule 19, pp. 60–62.

75 W. Boothby, above note 14, p. 233.

76 Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge University Press, Cambridge, 2004, p. 59 (emphasis added).

that would allow a robot such a determination [of proportionality], and nor is there any known metric to objectively measure needless, superfluous or disproportionate suffering. They require human judgement'.[77] This raises an issue specific to autonomous and remote weapons systems; presently a person must be sufficiently involved in the decision-making loop to satisfy the proportionality criterion.

Combining discrimination and proportionality with regard to the current methods of warfare in which autonomous and remote weapons systems are embedded raises significant questions of legality. The inability to comply with the rules of discrimination and proportionality is particularly apparent in recent instances of targeted killings conducted with remote weapons systems. Similarly, autonomous and remote weapons systems may have difficulties in recognizing *hors de combat* status as a result of poor sensing and computational ability; this may result in further violence being inflicted upon individuals who are *hors de combat* (or seek to be, by surrender) and, therefore, in violation of the IHL prohibition of the Denial of Quarter.[78]

Situating the legality of autonomous and remote weapons systems

In order to fully address the legality question of autonomous and remote weapons systems it is essential to consider how they are currently used.[79] While autonomous and remote weapons systems may not be inherently unlawful, the ways they are used may be. If such weapons systems are persistently implicated in legally controversial practices, however, it may justify a reconsideration of the legality question. Three especially pertinent uses and challenges are raised below.

Targeted killings and remote weapons systems[80]

Despite the controversy surrounding the practice of targeted killings, there is currently no commonly accepted definition. A former Legal Advisor for the International Committee of the Red Cross suggested that 'targeted killing' denotes 'the use of lethal force attributable to a subject of international law with the intent, premeditation and deliberation to kill individually selected persons who are not in the physical custody of those targeting them'.[81] The controversial legality of this practice was highlighted by Philip Alston, the former UN Special Rapporteur on

77 N. Sharkey, above note 67, p. 88.
78 J.-M. Henckaerts and L. Doswald-Beck, above note 44, Rule 46, p. 162; Rule 47, p. 164, and Rule 65, p. 225.
79 C. Pilloud *et al.*, above note 32, para. 1402.
80 There is evidence that the US is creating a global apparatus to carry out targeted killings. See Greg Miller, 'Under Obama, an emerging global apparatus for drone killing', in *The Washington Post*, 28 December 2011, available at: http://www.washingtonpost.com/national/national-security/under-obama-an-emerging-global-apparatus-for-drone-killing/2011/12/13/gIQANPdILP_story.html (last visited 18 January 2012).
81 Nils Melzer, *Targeted Killing in International Law*, Oxford University Press, Oxford, 2008, p. 5.

extrajudicial, summary or arbitrary executions, in his challenge to the US government to provide the legal basis upon which these take place:

> Targeted killings carried out by drone attacks on the territory of other States are increasingly common and remain deeply troubling. The US Government should disclose the legal basis for such killings and identify any safeguards designed to reduce collateral civilian casualties and ensure that the Government has targeted the correct person.[82]

Less than a year later, Harold Koh, the Legal Advisor to the US Department of State, replied with the unequivocal position held by the Obama Administration:

> What I can say is that it *is the considered view of this Administration – and it has certainly been my experience during my time as Legal Adviser – that US targeting practices, including lethal operations conducted with the use of unmanned aerial vehicles, comply with all applicable law, including the laws of war*.[83]

It is beyond the scope of this article to consider the validity of Harold Koh's assertion regarding US targeting practices.[84] Rather, the pertinent question concerns the review of the legality of using autonomous and remote weapons systems in a sustained campaign to kill suspected terrorists extraterritorially.[85] In other words, while autonomous and remote weapons systems may generally be capable of fulfilling the legality requirements for new weapons, their use in the context of targeted killings campaigns may not have been considered during the initial legal review. While Article 36 of Additional Protocol I requires States 'to determine whether its employment would, *in some or all circumstances*, be prohibited' the Commentaries specify that 'the article is intended to require States to analyse whether the employment of a weapon for its normal or expected use would be prohibited under some or all circumstances. A State is not required to foresee or analyse all possible misuses of a weapon, for almost any weapon can be misused in ways that would be prohibited'.[86] However, the position of this current author is that insofar as remote weapons systems can be considered as weapons, and have

82 Philip Alston, 'Statement by Professor Philip Alston, Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions', United Nations Human Rights Council Geneva, 3 June 2009, available at: http://www.un.org/webcast/unhrc/11th/statements/Alston_STMT.pdf (last visited 18 January 2012).

83 Harold Koh, 'The Obama Administration and international law', Annual Meeting of the American Society of International Law, Washington, DC, 25 March 2010, available at: http://www.state.gov/s/l/releases/remarks/139119.htm (last visited 20 December 2010).

84 Christof Heyns, however, has raised doubts about the legality of targeted killing practices used by the United States, stating that 'mere reference to a statement made by a senior State official is insufficient'. Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Christof Heyns, Addendum Follow-up to country recommendations – United States of America, UN Doc. A/HRC/20/22/Add.3, 30 March 2012, paras. 76-84, especially para. 79.

85 Targeted killings outside of the context of armed conflict or within the territory of the state itself are unlikely to be lawful. Philip Alston, 'Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Philip Alston: Addendum Study on Targeted Killings', UN Doc A/HRC/14/24/Add.6. 25, 2010, available at: http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf (last visited 18 January 2012). This article does not consider other situations that are not governed by IHL.

86 Additional Protocol I of 1977, Art. 36 (emphasis added). C. Pilloud *et al*., above note 32, para. 1469.

become inextricably associated with the policy of targeted killings, Article 36 would require a reappraisal of their legality because '[their] normal or expected use' would be transformed when used as implements that enable a legally controversial practice.

There are three specific legal questions that, although inherent to the practice of targeted killings, are made more complex by the use of autonomous and remote weapons systems. The first is the requirement of distinction between military and civilian targets, which is challenged by the labelling of the targets as 'suspected terrorists'. In an armed conflict, persons in this perceived category are prima facie civilians and are protected as such except when and for as long as they participate directly in hostilities; in non-international armed conflict specifically, individuals considered as members of organized armed groups having a 'continuous combat function' can be targeted at all times.[87] The uncertainties surrounding the ability of remote weapons systems to discriminate between legitimate military targets and non-military targets raise serious concerns about the erosion of the protection of civilians.

The second is the related question of proportionality in the use of force to prevent excessive force from being directed at civilians or civilian objects. This consideration is all the more important in this context because the suspected 'terrorists' being targeted are likely to intermingle with civilians or to be in the midst of civilian objects. Targeted killings by remotely controlled UAVs have reportedly been responsible for large numbers of casualties.[88] While the official Central Intelligence Agency (CIA) statistics claim a clean record with zero civilian casualties, this claim is the subject of considerable dispute.[89] This provides some factual basis for the contention that the use of autonomous and remote weapons systems in pursuit of a regime of targeted killings is unlawful on the grounds that it fails the requirements imposed by discrimination and proportionality.

The third legal question is the inevitability of disproportionate force associated with the denial of surrender or *hors de combat* status of the target.[90] There are difficulties inherent in attempting to surrender to remote weapons systems, but these may be overcome, as in an example provided by P. W. Singer where Iraqi combatants effectively surrendered to an American remotely controlled UAV in the first Gulf War.[91] The question rather is whether the intention to surrender or *hors de combat* status would be recognized by more autonomous weapons systems where human attention becomes increasingly alienated and

87 ICRC, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, Nils Melzer (ed.), ICRC, May 2009, pp. 70–71.

88 International Human Rights and Conflict Resolution Clinic (Stanford Law School) and Global Justice Clinic (NYU School of Law), *Living Under Drones: Death, Injury, and Trauma to Civilians from US Drone Practices in Pakistan*, September 2012; see also, BBC News, above note 11.

89 Scott Shane, 'C.I.A. is disputed on civilian toll in drone strikes', in *The New York Times*, 11 August 2011, available at: http://www.nytimes.com/2011/08/12/world/asia/12drones.html?hp (last visited 12 January 2012).

90 N. Melzer, above note 81, pp. 368–370.

91 P. W. Singer, above note 7, pp. 56–57.

removed. Finally, the question of surrender to an autonomous or remote weapons system raises a technical legal issue: the institution of surrender is one between rival combatants. As a combatant cannot surrender to the weapons of the opposing side alone, this raises questions as to the possibility of surrendering to such a system, or conversely, whether either autonomous or remote weapons systems can coherently be categorized as mere weapons.

The civilianization of military force

Military and strategic history has been characterized by attempts by the state and its military establishments to monopolize the material and technological means through which organized force is deployed.[92] The ambiguous status of autonomous and remote weapons systems is starkly illustrated by the lack of control in its development, production, and distribution in contradistinction to this monopolizing tendency; indeed, the rapid technological advancement in the area of military robotics has not, paradoxically, been accompanied by attempts to regulate its use or distribution. In part this may be due to the fact that civilian research and development underlies much of the relevant technology and the production of the actual machinery occurs in civilian facilities. Furthermore, civilians are intricately involved in the maintenance and actual use of these systems.[93] Thus, attempts by the military establishment to monopolize the associated technology or capability may be futile.

The heavy involvement of civilians in all stages of autonomous and remote weapons system development, production, maintenance, and use may significantly widen the category of legitimate military objective. First, this creates a potentially wide category of dual-use facilities where autonomous and remote weapons are being designed, or produced, for both civilian and military functions. The text of Article 52(2) of Additional Protocol I may be understood to enable the classification of all dual-use facilities as legitimate military targets.[94] Second, civilians operating autonomous and remote weapons systems are likely to lose their immunity from direct attack for the duration of their direct participation in hostilities and will thus be susceptible to domestic prosecution.[95] It is also important to note that this legalistic consideration regarding legitimate military targets may overshadow the tendency towards civilians bearing the brunt of the adverse effects of contemporary armed conflict in reality. This may in turn create pressure to target civilians and civilian objects in lieu, especially taking into account the increased direct participation in hostilities of the former and the dual-use of the latter.

92 Alexander Gillespie, *A History of the Law of War: The Customs and Laws of War with Regards to Arms Control*, Hart, Oxford, 2011, pp. 7–78.

93 David S. Cloud, 'Civilian contractors playing key roles in US drone operations', in *The Los Angeles Times*, 29 December 2011, available at: http://www.latimes.com/news/nationworld/world/la-fg-drones-civilians-20111230,0,6127185.story (last visited 18 January 2012).

94 Henry Shue and David Wippman, 'Limiting attacks on dual-use facilities performing indispensible civilian functions', in *Cornell International Law Journal*, Vol. 35, 2001–2002, p. 562.

95 See generally, N. Melzer, above note 87, pp. 41–68.

Aside from purely IHL considerations, the infiltration of military force into the civilian sphere may engender the creep of militarization into law enforcement and policing.[96] Furthermore, the ready availability of this technology enables broad access: anti-whaling campaigners, for example, have deployed surveillance drones to spot a Japanese whaling fleet, and 'drones and other types of unmanned aerial vehicles [. . .] are being sent on civilian missions such as crop inspections or marine mammal surveys'.[97] Indeed, civilian applications for drone technology are seen in the United States as inevitable, and the Federal Aviation Administration is to propose new rules to integrate small drones into national airspace.[98] While it must be emphasized that these systems are not currently weaponized, and therefore not within the ambit of autonomous and remote weapons systems, it should also be noted in this context that the unmanned military systems were initially deployed for surveillance purposes and were only weaponized subsequently. It may therefore not be surprising if drones in the civilian sphere, such as those to be used by police, were to be weaponized at a later stage, leading to the subtle militarization of the civilian sphere.

Cyberwarfare: blurring the lines between the virtual and real worlds

The deployment of autonomous and remote weapons systems may allow the conduct of cyberwarfare to have very concrete and real-world effects. An emerging field,

> cyberwarfare is the conduct of military operations by virtual means. It consists of nation-states' using cyberspace to achieve essentially the same ends they pursue through the use of conventional military force: achieving advantages over a competing nation-state or preventing a competing nation-state from achieving advantages over them.[99]

Currently, this form of military conflict exists primarily in 'information warfare units to develop viruses to attack enemy computer systems and networks, and tactics . . . to protect friendly computer systems and networks'.[100] Thus, cyberwarfare is correctly termed; it cannot yet be considered a form of armed conflict because

96 Brian Bennett, 'Police employ Predator drone spy planes on home front', in *The Los Angeles Times*, 10 December 2011, available at: http://articles.latimes.com/2011/dec/10/nation/la-na-drone-arrest-20111211 (last visited 18 January 2012).

97 Jonathan Franklin, 'Whaling: campaigners use drones in the fight against Japanese whalers', in *The Guardian*, 1 January 2012, available at: http://www.guardian.co.uk/environment/2012/jan/01/drones-fight-japanese-whalers (last visited 18 January 2012).

98 W. J. Hennigan, 'Idea of civilians using drone aircraft may soon fly with FAA', in *The Los Angeles Times*, 27 November 2011, available at: http://articles.latimes.com/2011/nov/27/business/la-fi-drones-for-profit-20111127 (last visited 18 January 2012).

99 Susan Bremner, *Cyberthreats: The Emerging Fault Lines of the Nation State*, Oxford University Press, Oxford, 2009, p. 65.

100 Office of the Secretary of Defense, 110th Congress, Annual Report to Congress: Military Power of the People's Republic of China, 2007, p. 22, available at: http://www.defenselink.mil/pubs/china.html (last visited 18 January 2012).

it remains exclusively within the virtual realm of cyberspace but bears many of the other hallmarks of warfare. This is because the aim of cyberwarfare is 'to get the upper hand of the enemy in a war under conditions of informatization . . . whether or not we are capable of using various means to obtain information and of ensuring the effective circulation of information'.[101]

While conduct in cyberspace may have significant and pervasive effects in the real world, it is the emergence of autonomous and remote weapons systems that may directly incorporate cyberwarfare (along with its lower-threshold counterparts of cybercrime and cyberterrorism) into armed conflict in the physical world. This is because the computer systems underlying both autonomous and remote weapons systems are especially vulnerable to cyberattack, which may in turn mean that these weapons systems may be hijacked for the purposes of perpetrating a physical attack in the real world. This has already been revealed in the recent 'Keylogger' computer virus infection at Creech Air Base in Nevada.[102] While it is uncertain whether or not this was actually a directed attack, and while it appeared benign, the vulnerability of both autonomous and remote weapons systems was clearly demonstrated. With the specific vulnerability of these systems to cyberattack in mind, the recent Iranian claims to have brought down an advanced US stealth drone by hacking into its systems underline the potential dangers of cyberattacks having real world repercussions.[103]

These cyberspace issues are further compounded by difficulties surrounding responsibility for the actions of autonomous and remote weapons systems. There are two main limbs to the challenge of responsibility. The first is simply that the control of even a strictly remotely controlled weapons system may constantly be under doubt because of the possibility that its information systems have been compromised. This raises questions about whether it will be possible to definitively attribute responsibility over such a system to its controller.[104] The second difficulty stems from the nature of cyberwarfare itself. Leaving aside the additional difficulties associated with cybercrime and cyberterrorism, unlike 'the physical world, when a country is at war, it knows it is at war and, most likely, with whom' when it comes to cyberwarfare it may be impossible to ascertain 'who was responsible for the attacks or why they were launched'.[105] While this engenders serious concern for cyberspace, the potential for real world violence to be unleashed through the anonymity of cyberspace is likely to create impunity for potentially grave violations of international humanitarian and human rights law.

101 Quoting a Liberation Army Commentator, *ibid*., p. 21.

102 Associated Press, 'Computer virus infects drone plane command centre in US', in *The Guardian*, 9 October 2011, available at: http://www.guardian.co.uk/technology/2011/oct/09/virus-infects-drone-plane-command (last visited 18 January 2012).

103 Agence France-Presse, 'Iran to "reverse-engineer" seized stealth drone after hacking operating system', in *The National Post*, 12 December 2011, available at: http://news.nationalpost.com/2011/12/12/iran-to-reverse-engineer-u-s-stealth-drone/ (last visited 18 January 2012).

104 In other words, will the controller of such a system have the capacity to be responsible for the actions of the system? Clearly, this issue is magnified if the system possesses any level of autonomy.

105 S. Bremner, above note 99, p. 7.

INTERNATIONAL REVIEW of the Red Cross

Superiority of autonomous and remote weapons systems and the responsibility question

As the potential failings of autonomous and remote weapons systems have been addressed, their potential to outperform their human counterparts in discrimination and proportionality tasks must equally be considered. The roboticist Ronald Arkin is optimistic that robotic lethality may be suitably governed to the point that both autonomous and remote weapons systems may outperform humans.[106] Similarly, in relation to the discrimination criterion, Justin McClelland writes:

> One area that will need careful consideration is the application of the criteria of distinction to the employment of 'autonomous' weapons. Such weapons have the capability, to varying degrees, to make decisions without any human involvement on the identification and attack of targets. This absence of what is called a 'man in the loop' does not necessarily mean that the weapon is incapable of being used in a manner consistent with the principle of distinction. The target detection, identification and recognition phases may rely on sensors that have the ability to distinguish between military and non-military targets. *By combining several sensors the discriminatory ability of the weapon is greatly enhanced*.[107]

The precise determination of legality with regard to discrimination will depend upon the characteristics of the system itself, but it should be noted here that the potential for increased sensory ability may be irrelevant if the computational system evaluating the data input is incapable of making an appropriate analysis, as Noel Sharkey has suggested.[108]

Ronald Arkin notes further that autonomous and remote weapons systems may be capable of better adherence to IHL compared to human combatants.[109] For example, these weapons systems may be able to combine the input from an array of sensory data to assess the threat and confirm the target, and it may be possible to programme the weapons system to refrain from attack despite risk to itself until a higher degree of certainty is ascertained to meet the principle of discrimination. Similarly, autonomous and remote weapons systems may be equipped with non-lethal weaponry in combination with discrimination precautions to rebalance the proportionality consideration. Finally, such systems will be resilient to adverse psychological effects that underlie the perpetration of some unlawful acts by human actors.

Thus, while Ronald Arkin may be correct that machines may possess a greater capacity to adhere to IHL, which may also in turn incentivize human soldiers

106 R. Arkin, above note 8, 2009, pp. 29–36 and 211–212.

107 J. McClelland, above note 34, pp. 408–409 (emphasis added).

108 N. Sharkey, above note 67, pp. 87–88. Not only is there a need for 'a clear computational definition of a civilian, [but] we would still need all of the relevant information to be made available from the sensing apparatus . . . These may be able to tell us that something is a human, but they would not be able to tell us much else'.

109 R. Arkin, above note 8, pp. 29–30.

to respect IHL, this approach neglects the fundamental consideration of responsibility for their breach. Peter Cane writes that responsibility looks in both temporal directions, historic and prospective; the former concerns notions of accountability for actions after the fact, while the latter serves to delineate obligations and duties before the fact.[110] Applying this idea of responsibility to the current discussion, it is clear that the greater capacity for adhering to IHL by autonomous and remote weapons systems is exclusively prospective in outlook. This is because only the obligation or duty to adhere to the relevant legal requirements can be programmed into the weapons system. Notions of historic responsibility are simply inapplicable under current legal understandings. In other words, while a higher level of obligation or prospective responsibility to adhere to IHL may be programmed into autonomous and remote weapons systems, it will be difficult if not impossible to attribute historic legal accountability if this law is breached. The potential for impunity arising from the use of such weapons systems is thus readily apparent.

The difficulty associated with historic responsibility is further compounded by possible attempts to attribute such responsibility. Although there is the potential that artificial decision-making may elevate its ontological level, the concomitant questions raised for responsibility have not been settled. Clearly, both the purpose and appropriateness of punishing a machine are questionable. Relocating the locus of punishment to natural persons with the closest nexus to these machines, however, runs the risk of scapegoating those persons: the possession of autonomous decision-making capacity may break the causal chain that would justify the attribution of responsibility to those persons. Thus, autonomous and remote weapons systems may have a higher capacity to adhere to IHL, but will inevitably have much lower levels of responsibility for any breaches. This leads to impunity for conduct in armed conflict.

The problems associated with responsibility are further compounded by the atomized approach of the law to questions of responsibility; that is, that it seeks to attribute responsibility to a concrete and definable entity for the creation of some specified effect. This runs contrary to the development of networks and swarms.[111] This has implications for responsibility for autonomous and remote weapons systems, as Mark Coeckelbergh explains:

> In a network, (military) activity is not about single, atomistic agents exercising their agency in single actions. Instead, agency (if this is still the adequate term at all) is distributed, collective, and emergent. It cannot be reduced to the level of the parts (systems metaphor), nodes (network metaphor), or – why not – 'bees' (swarms metaphor). None of the parts, nodes, or bees control the action (in this sense they are not agents), but the system, network, or swarm as a whole acts.[112]

110 Peter Cane, *Responsibility in Law and Morality*, Oxford University Press, Oxford, 2002, pp. 31–34.
111 M. Coeckelbergh, above note 41, p. 273.
112 *Ibid.*

Thus, current conceptions of legal responsibility may be wholly inadequate to address the questions raised by the rise of autonomous and remote weapons systems. This inadequacy becomes all the more important when the outcomes of the use of these weapons systems rise to the level of international crimes.

Conclusion

While this article has focused on the many potential pitfalls arising from the emergence of autonomous and remote weapons systems, it is necessary to emphasize their potential to reinforce humanitarian principles and enable a closer adherence to IHL. Ronald Arkin is certainly correct in highlighting the potential superiority of autonomous and remote systems vis-à-vis human frailties in situations of armed conflict. Moreover, the utility of these systems continues to be demonstrated, which guarantees their future in the battlespace.

It is, however, easy to be blinded by the combined apparent superiority and inevitability of autonomous and remote weapons systems so that IHL fails to fully realize the categorical departure that is signalled by their arrival. As David Kennedy has pointed out, 'humanitarian rules may well criticize too little – relying for their implementation on the agreement of the military and political establishments which collectively promulgate them. Waging war within the rules may so little constrain the use of force that adherence to humanitarian rules will do more to legitimate than contain force.'[113] As discussed above, the continued applicability of IHL to these novel weapons, means and methods of warfare is apparent. The problem, however, is that IHL provides guiding principles rather than clearly defined rules and regulations. Again, David Kennedy speaks of the problem that this creates: 'Humanitarian standards seem too vague to restrain those determined to use force, too manipulable to embody humanitarian commitments. In the chaos of war, it seems unlikely that anything other than a clear rule will function'.[114]

The development of autonomous and remote weapons systems is currently in its infancy, so Kennedy's critique based on international humanitarian standards need not apply. It is still possible at this stage to articulate rules that are directly applicable to the use of these weapons systems, as well as to delineate the boundaries of permissibility for their future development. The important questions of responsibility need neither be ignored nor neglected until a watershed catastrophe compels their consideration, and establishing the limits and the modalities to attribute responsibility now will limit the scope for future impunity. Finally, the pronouncement of applicable rules needs to be accompanied by monitoring and enforcement mechanisms. This will present a significant hurdle because states are unlikely to impose limitations upon themselves in instances where they possess, or are in the process of developing, means and methods of warfare that are likely to confer military superiority. As Theodor Meron warns: 'The tremendous progress in

113 David Kennedy, *The Dark Sides of Virtue: Reassessing International Humanitarianism*, Princeton University Press, Princeton, 2004, pp. 296–297.
114 *Ibid.*, p. 297.

the humanization of the law of war brings into sharp relief the stark contrast between promises made in treaties and declarations . . . on the one hand, and the harsh, often barbaric practices actually employed on the battlefield'.[115] The humanity of IHL is jeopardized not only by the emergence of autonomous and remote weapons systems, but also by the failure to recognize these as being categorically different from preceding weapons and by not recognizing their potential to drastically alter the existing legal category of means and methods of warfare.

This article has argued that contemporary IHL is insufficient to regulate some technologically advanced weapons systems, and that the current legal categorization is challenged by the emergence of autonomous weapons systems that possess autonomous capabilities. Insofar as both autonomous and remote weapons systems do not adequately fit into current categories of IHL, it may be that these systems should constitute a novel common category. Both autonomous and remote weapons systems do not fit squarely within the legal understanding of a weapon, and create subtle, yet fundamental, changes to the current legal understanding of means and methods of warfare. It may therefore be inappropriate to expand the existing categories to encompass these advanced weapons systems. Instead, it is likely that new rules will need to be developed to ensure that the potential superiority, in humanitarian terms, of these advanced weapons systems is harnessed and that concomitant responsibility for their use is firmly established to incentivize compliance and to forestall allegations of impunity. The need to establish an architecture of responsibility for the use of autonomous and remote weapons systems becomes especially acute where their use leads to allegations of international crimes.

115 Theodore Meron, *The Humanization of International Law*, Martinus Nijhoff, Leiden, 2006, p. 85.

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

Nanotechnology and challenges to international humanitarian law: a preliminary legal assessment

Hitoshi Nasu*

Hitoshi Nasu is Senior Lecturer in law at the Australian National University, Canberra, Australia.

Abstract

The introduction of nanotechnology into our civil life and warfare is expected to influence the application and interpretation of the existing rules of international humanitarian law. This article examines the challenges posed to international humanitarian law by the widespread use of nanotechnology in light of four basic rules of international humanitarian law: (1) the obligation to ensure the legality of weapons; (2) distinction; (3) proportionality; and (4) precaution. It concludes by identifying three areas of concern, which arise from widespread use of nanotechnology, for the application of international humanitarian law.

Keywords: nanotechnology, superfluous injury or unnecessary suffering, environmental protection, the principle of distinction, proportionality, precaution.

* The author thanks Associate Professor Robert McLaughlin, Professor Ken Watkin, CAPT Andy Norris, CAPT (Ret.) Dennis Mandsager, Lt Col. George Cadwalader, MAJ Matt Hover, Ms Sasha Radin, Professor Tom Faunce, and anonymous reviewers for their invaluable comments on an earlier draft, and Rosanna Bartlett, David Rowe, and Pauline Wilson for their research assistance. The author also gratefully acknowledges the support of the Australian Research Council under its Discovery Grant funding scheme (Project ID110102637).

doi:10.1017/S181638311200077X

The interaction between technological development and armed forces is a constant feature of the history of warfare. Technological development can be stimulated by, and dedicated directly to addressing, military requirements. On other occasions, technological development outside the military sphere affects or informs the conduct of warfare and military expectations, as has been illustrated by the application of computing and software innovations that have led to major changes in the military tactics of developed nations.[1] Nanotechnology is widely considered a next-generation transformational technology with profound implications for all aspects of modern society.[2] The introduction of nanotechnology into our civil life and warfare is also expected to influence the application and interpretation of the existing rules of international humanitarian law, raising 'the question of whether the rules are sufficiently clear in light of the technology's specific characteristics, as well as with regard to the foreseeable humanitarian impact it may have'.[3]

This article examines the challenges posed to international humanitarian law by the widespread use of nanotechnology-enabled materials and other potential applications of nanotechnology in light of what is feasible at the present stage of scientific research.[4] This assessment can only be preliminary because the full potential of nanotechnology is yet to be revealed. To that end, the article first introduces various applications of nanotechnology relevant to the conduct of modern warfare with a particular focus on armed attacks by conventional weapons.[5] It then examines the impact and influence of nanotechnology for the application of four basic rules of international humanitarian law. It concludes by identifying three

1 See generally, Peter Dombrowski and Eugene Gholz, *Buying Military Transformation: Technological Innovation and the Defense Industry*, Columbia University Press, New York, 2006; Henry C. Bartlett *et al.*, 'Force planning, military revolutions and the tyranny of technology', in *Strategic Review*, Vol. 24, No. 4, Fall 1996, pp. 28–40.

2 See e.g., the Center for International Environmental Law (CIEL), *Addressing Nanomaterials as an Issue of Global Concern*, May 2009, p. 1, available at: http://www.ciel.org/Publications/CIEL_NanoStudy_May09.pdf (last visited 30 October 2012).

3 International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, Report on the 31st International Conference of the Red Cross and Red Crescent, Geneva, 28 November–1 December 2011, p. 36, available at: http://www.icrc.org/eng/resources/documents/report/31-international-conference-ihl-challenges-report-2011-10-31.htm (last visited 30 October 2012). For an earlier study on the impact of technology in general on international humanitarian law, see especially, Michael N. Schmitt, 'War, technology and the law of armed conflict', in Anthony M. Helm (ed.), *The Law of War in the 21st Century: Weaponry and the Use of Force*, US Naval War College International Law Studies, Vol. 82, Naval War College, Newport, 2006, p. 137.

4 Thus, this article does not concern futuristic, speculative applications of nanotechnology, such as universal molecular assemblers and autonomous nano-robots, though some of the findings in this article may well be applicable to them. For a comprehensive account of scientifically possible applications of nanotechnology, see, e.g., Jürgen Altmann, *Military Nanotechnology*, Routledge, London, 2006; Jun Wang and Peter J. Dortmans, 'A review of selected nanotechnology topics and their potential military applications', Defence Science and Technology Organisation, Australian Government Department of Defence, 2004, pp. 22–30, available at: http://www.dsto.defence.gov.au/publications/2610/DSTO-TN-0537.pdf (last visited 30 October 2012).

5 The application of nanotechnology for biological, chemical, or nuclear weapons requires a separate legal analysis by reference to relevant treaty regimes and is therefore excluded from the focus of this article.

areas of concern arising from widespread use of nanotechnology for the application of international humanitarian law.

The relevance of nanotechnology to warfare

Nanotechnology is a rapidly evolving field of science cutting across many disciplines including engineering, quantum physics, optics, chemistry, and biology, and typically involves manipulation of matter on the atomic and molecular level in the size range of 1 nm – 100 nm (1 nm = 10^{-9}m) in one or more external dimensions.[6] Engineered nanomaterials (ENMs) and nanoparticles (ENPs) possess unique characteristics such as flame-retardation, dirt-resistance, increased electrical conductivity, and improved hardness and strength with reduced weight, which have proven to be popular for applications in a wide range of commercially marketed products.[7]

At the same time, however, concerns have been raised about potential toxicity for human health and biological and environmental systems.[8] While no conclusive toxicity profile for engineered nanomaterials and nanoparticles is yet available, there is already compelling scientific evidence of human and environmental toxicity in relation to certain ENMs and ENPs. Examples include the toxicity of multi-walled carbon nanotubes,[9] silver nanomaterials ('nanosilver'),[10] titanium dioxide nanoparticles,[11] nanoparticle zinc powder,[12] cobalt nanoparticles,[13] and

6 For different definitions of nanotechnology, see, e.g., European Commission, Commission Recommendation on the definition of nanomaterial, available at: http://ec.europa.eu/environment/chemicals/nanotech/pdf/commission_recommendation.pdf (last visited 30 October 2012); US Environmental Protection Agency (EPA), *Nanotechnology White Paper*, Office of the Science Advisor, EPA 100/B-07/001, February 2007, p. 5, available at: http://www.epa.gov/osa/pdfs/nanotech/epa-nanotechnology-whitepaper-0207.pdf (last visited 30 October 2012).

7 The Project on Emerging Nanotechnologies at the Woodrow Wilson International Center for Scholars regularly updates an inventory of nanotechnology consumer products, which is available at: http://www.nanotechproject.org/inventories/consumer/ (last visited 30 October 2012).

8 See, e.g., US EPA, above note 6, pp. 29–62; UK Department for Environment, Food and Rural Affairs, 'Characterising the potential risks posed by engineered nanoparticles: a second UK government research report', 2007, available at: http://www.defra.gov.uk (last visited 30 October 2012); UK Royal Society & Royal Academy of Engineering, *Nanoscience and Nanotechnologies: Opportunities and Uncertainties*, 2004, available at: http://www.nanotec.org.uk/finalReport.htm (last visited 30 October 2012).

9 See, e.g., Massimo Bottini *et al.*, 'Multi-walled carbon nanotubes induce T lymphocyte apoptosis', in *Toxicology Letters*, Vol. 160, 2006, pp. 121–126.

10 See, e.g., Maqusood Ahamed, Mohamad S. Alsalhi and M. K. J. Siddiqui, 'Silver nanoparticle applications and human health', in *Clinica Chimica Acta*, Vol. 411, 2010, pp. 1841–1848; Susan W. P. Wijnhoven *et al.*, 'Nano-silver – a review of available data and knowledge gaps in human and environmental risk assessment', in *Nanotoxicology*, Vol. 3, No. 2, 2009, pp. 109–138.

11 See, e.g., Benedicte Trouiller *et al.*, 'Titanium dioxide nanoparticles induce DNA damage and genetic instability in vivo in mice', in *Cancer Research*, Vol. 69, No. 22, 2009, pp. 8784–8789.

12 See, e.g., Bing Wang *et al.*, 'Acute toxicity of nano- and micro-scale zinc powder in healthy adult mice', in *Toxicology Letters*, Vol. 161, No. 2, 2006, pp. 115–123.

13 See, e.g., Limor Horev-Azaria *et al.*, 'Predictive toxicology of cobalt nanoparticles and ions: comparative *in vitro* study of different cellular models using methods of knowledge discovery from data', in *Toxicological Sciences*, Vol. 122, No. 2, 2011, pp. 489–501.

nickel nanoparticles.[14] Those ENMs and ENPs, when inhaled, typically elicit pulmonary inflammation and cardiovascular problems.[15] Scientific studies have also suggested carcinogenicity, cytotoxicity, and genotoxicity of certain nanomaterials and nanoparticles.[16] These health and environmental hazards are not localized because of the potential long-range transport of nanoparticles through the air and water after their release into the environment.[17]

The relevance of nanotechnology to the military resides particularly in its application to enhance military capabilities including:

- soldier survivability (for example, lighter, stronger, and heat-resistant armour and clothing);[18]
- force protection (for example, enhanced camouflaging,[19] undetectable coating of aircrafts,[20] explosive detectors,[21] bio/chemical sensors[22]);
- force mobility (for example, miniaturization of communication devices,[23] increased energy generation and storage capacity[24]);

14 See, e.g., Jodie R. Pietruska *et al.*, 'Bioavailability, intracellular mobilization of nickel, and HIF-1α activation in human lung epithelial cells exposed to metallic nickel and nickel oxide nanoparticles', in *Toxicological Sciences*, Vol. 124, No. 1, 2011, pp. 138–148.

15 See, e.g., Weiyue Feng *et al.*, 'Nanotoxicity of metal oxide nanoparticles *in vivo*', in Saura C. Sahu and Daniel A. Casciano (eds), *Nanotoxicology: From In Vivo and In Vitro Models to Health Risks*, John Wiley & Sons, West Sussex, 2009, pp. 247–269; Ken Donaldson *et al.*, 'Pulmonary and cardiovascular effects of nanoparticles', in Nancy A. Monteiro-Riviere and C. Lang Tran (eds), *Nanotoxicology: Characterization, Dosing and Health Effects*, Informa Healthcare, New York, 2007, pp. 267–298; Günter Oberdörster *et al.*, 'Nanotoxicology: an emerging discipline evolving from studies of ultrafine particles', in *Environmental Health Perspectives*, Vol. 113, No. 7, 2005, pp. 829–833.

16 See generally, Shareen H. Doak *et al.*, 'Genotoxicity and cancer', in Bengt Fadeel *et al.*, (eds), *Adverse Effects of Engineered Nanomaterials: Exposure, Toxicology, and Impact on Human Health*, Elsevier, London, 2012, pp. 243–261; Laetitia Gonzalez, Dominique Lison and Micheline Kirsch-Volders, 'Genotoxicity of engineered nanomaterials: a critical review', in *Nanotoxicology*, Vol. 2, No. 4, 2008, pp. 252–273.

17 CIEL, above note 2, pp. 11–12.

18 The Institute for Soldier Nanotechnologies (ISN) was established as a centre for research collaboration between the US Army and the Massachusetts Institute of Technology to conduct basic and applied research to enhance soldier survivability, see the website at: http://web.mit.edu/ISN/ (last visited 30 October 2012).

19 See, e.g., Andrea Di Falco, Martin Ploschner and Thomas F. Krauss, 'Flexible metamaterials at visible wavelengths', in *New Journal of Physics*, Vol. 12, 2010, p. 113006.

20 See, e.g., Haofei Shi *et al.*, 'Low density carbon nanotube forest as an index-matched and near perfect absorption coating', in *Applied Physics Letter*, Vol. 99, 2011, p. 211103.

21 See, e.g., I. A. Levitsky, 'Highly sensitive and selective explosive detector based on nanoporous silicon photonic crystal infiltrated with emissive organics', in *IEEE Nanotechnology Magazine*, September 2010, p. 24.

22 For a detailed analysis, see Margeret E. Kosal, *Nanotechnology for Chemical and Biological Defense*, Springer, Dordrecht, 2009, pp. 43–52.

23 J. Wang and P. J. Dortmans, above note 4, p. 28.

24 The US Department of Defense identified electrochemical power source applications of nanotechnology as one of the primary goals of its nanotechnology research and development programme. See US Department of Defense, 'Defense nanotechnology research and development program', 2007, available at: http://www.fas.org/irp/agency/dod/nano2007.pdf (last visited 30 October 2012).

- penetration capability (for example, nano-energetic explosives,[25] armour-piercing projectiles coated with a nano-material[26]); and
- focused force application (for example, 'nano air vehicles',[27] self-guiding bullets[28]).

Thus, military applications of nanotechnology extend to both offensive and defensive capabilities. Even purportedly defensive applications, such as enhanced armour and camouflage, provide certain operational and tactical advantages, which could have implications for the interpretation and application of the existing rules of international humanitarian law.

Widespread use of nanotechnologies in commercially marketed products also means that military operations in the modern environment may involve targeting nanotechnology-enabled products or destroying them as collateral damage. For example, building materials may contain nanotechnology-enabled products, such as thermal insulation coating, anti-bacterial paint, and self-cleaning glass.[29] Engineered metal nanomaterials are likely to be widely used for solar power plants and water filtration plants to enhance their capacity and efficiency.[30] Even if ENMs are firmly embedded in larger structures and are therefore difficult to separate from the structural components, strong physical impacts may well result in an accidental release of hazardous ENMs and ENPs when targeted by kinetic means or as a result of fire.[31] Upon release, ENMs and

25 Jefferson D. Raynolds, 'Collateral damage on the 21st century battlefield: enemy exploitation of the law of armed conflict, and the struggle for a moral high ground', in *Air Force Law Review*, Vol. 56, 2005, p. 99 (nano-energetics provide more effective control of blast, relying on nano-structured explosives and fuel additives, as well as catalytics and photovoltaics); Andrzej W. Miziolek, 'Nanoenergetics: an emerging technology area of national importance', in *Advanced Materials and Processes Technology Information Analysis Center (AMPTIAC) Newsletter*, Vol. 6, No. 1, 2002, p. 43.

26 An advanced armour-piercing projectile involving the potential use of NanoSteel™ is patented in the US: Daniel James Branagan, 'Layered metallic material formed from iron based glass alloys', The Nanosteel Company, Inc., US Patent 7482065, 21 April 2009, available at: http://www.freepatentsonline.com/7482065.html (last visited 30 October 2012).

27 The 'nano air vehicles' are extremely small, ultra-lightweight airborne vehicles capable of performing a military mission, developed by the US Defense Advance Research Projects Agency (DARPA). See, William A. Davis, 'Nano air vehicles: a technology forecast', Blue Horizons Paper, Center for Strategy and Technology, US Air War College, 2007, available at: http://www.au.af.mil/au/awc/awcgate/cst/bh_davis.pdf (last visited 30 October 2012).

28 Duncan Blake and Joseph S. Imburgia, '"Bloodless weapons"? The need to conduct legal reviews of certain capabilities and the implications of defining them as "weapons"', in *Air Force Law Review*, Vol. 66, 2010, p. 180.

29 See, e.g., Sabine Greßler and André Gazsó, 'Nano in the construction industry', in *NanoTrust Dossiers*, No. 32, 2012, available at: http://epub.oeaw.ac.at/ita/nanotrust-dossiers/dossier032en.pdf (last visited 1 November 2012).

30 See, e.g., Tao Chen *et al.*, 'Flexible, light-weight, ultrastrong, and semiconductive carbon nanotube fibers for a highly efficient solar cell', in *Angewandte Chemie International Edition*, Vol. 50, 2011, pp. 1815–1819; OECD, 'Fostering nanotechnology to address global challenges: water', 2011, available at: http://www.oecd.org/dataoecd/22/58/47601818.pdf (last visited 1 November 2012).

31 Grazyna Bystrzejewska-Piotrowska, Jerzy Golimowski and Pawel L. Urban, 'Nanoparticles: their potential toxicity, waste and environmental management', in *Waste Management*, Vol. 29, 2009, p. 2592. In fact, Canadian fire services consider released ENMs and ENPs to be serious health hazards. See, Ed Ballam, 'Nanotechnology spells danger for firefighters', in *Firehouse.com News*, 24 April 2012, available at: http://www.firehouse.com/news/10705138/nanotechnology-spells-danger-for-firefighters (last visited 30 October 2012).

ENPs may enter into human bodies through inhalation, and also into the environment with the real possibility that nanomaterials may move through food chains and culminate in human exposure.[32] Very little information is currently available on the potential longevity of ENMs and ENPs in the environment, bioaccumulation, and the possibility of detection and removal – particularly in relation to weathered nanoparticles that have undergone agglomeration and transformation.[33] Particularly when ENMs and ENPs are dispersed into the air and water, the risk of long-term, widespread, severe health and environmental damages cannot be easily dismissed.

Health and environmental concerns associated with the use of a particular type of weapon are not unique to nanotechnologies in modern warfare. Concern has been raised, for example, with regard to indirect impacts of metal dust in whatever form it might be released. Illustrative is the Gulf War Syndrome, which is thought to be caused by exposure to toxic chemicals released upon impact by depleted uranium weapons.[34] Scientific evidence also suggests the possibility that the energy-charged, heavy metal tungsten alloy (HMTA) powder released by dense inert metal explosives (DIME) is tumour-generating and capable of genotoxic effects.[35] One significant difference between such toxic chemicals and ENMs or ENPs, however, is that it is not just the military use in weaponry, but more importantly, the widespread civilian use that is likely to cause a large-scale release of toxic substances and hence significantly increase the risk of exposure.

Acknowledging a wide range of beneficial applications of nanotechnology, particularly in addressing national priority issues such as energy security and water

32 R. D. Handy and B. J. Shaw, 'Toxic effects of nanoparticles and nanomaterials: implications for public health, risk assessment and the public perception of nanotechnology', in *Health, Risk & Society*, Vol. 9, No. 2, 2007, pp. 125–144.

33 Stephen J. Klaine *et al.*, 'Paradigms to assess the environmental impact of manufactured nanomaterials', in *Environmental Toxicology and Chemistry*, Vol. 31, No. 1, 2012, pp. 3–14; Satinder K. Brar, Mausam Verma, R. D. Tyagi and R. Y. Surampalli, 'Engineered nanoparticles in wastewater and wastewater sludge – evidence and impacts', in *Waste Management*, Vol. 30, 2010, pp. 504–520; CIEL, above note 2; US EPA, above note 6, pp. 36–41.

34 Initially, no causal link was established. However, scientific evidence proving the hazardous effects of toxic chemicals released upon impact of deplete uranium weapons has continued to mount. For details, see, e.g., Dan Fahey, 'Environmental and health consequences of the use of depleted uranium weapons', in Avril McDonald, Jann K. Kleffner and Brigit Toebes (eds), *Depleted Uranium Weapons and International Law: A Precautionary Approach*, T. M. C. Asser Press, The Hague, 2008, pp. 29–72; Melissa A. McDiarmid *et al.*, 'Health effects of depleted uranium on exposed Gulf War veterans: a 10-year follow-up', in *Journal of Toxicology and Environmental Health*, Vol. 67, No. 4, 2004, pp. 277–296; The Royal Society Working Group on the Health Hazards of Depleted Uranium Munitions, 'The health effect of depleted uranium munitions: a summary', in *Journal of Radiological Protection*, Vol. 22, 2002, pp. 132–134.

35 See, e.g., Erik Q. Roedel *et al.*, 'Pulmonary toxicity after exposure to military-relevant heavy metal tungsten alloy particles', in *Toxicology and Applied Pharmacology*, Vol. 259, 2012, pp. 74–86; John F. Kalinich *et al.*, 'Embedded weapons-grade tungsten alloy shrapnel rapidly induces metastatic high-grade rhabdomyosarcomas in F344 rats', in *Environmental Health Perspective*, Vol. 113, 2005, pp. 729–734; Alexandra C. Miller *et al.*, 'Neoplastic transformation of human osteoblast cells to the tumorigenic phenotype by heavy metal tungsten alloy particles: induction of genotoxic effects', in *Carcinogenesis*, Vol. 22, 2001, pp. 115–125.

security, as well as strong interests in the development of nanotechnologies for businesses and industries, it is highly unlikely that national regulatory authorities will move to ban the use of ENMs and ENPs.[36] Nevertheless, some states have recently started regulating the use of ENMs and ENPs in consumer products based on their 'use scenario'.[37] Yet, national regulation will not effectively prevent toxic ENMs and ENPs, released as a result of armed attacks, from posing widespread health and environmental hazards unless the regulation is specifically designed for such an event.[38]

Nanotechnology and the principles of international humanitarian law

Currently there is no international treaty that specifically regulates the use of nanotechnology for military purposes or otherwise. A preventive arms control treaty to regulate or ban the use of nanotechnology for military purposes is unlikely to materialize[39] because international arms control treaties tend to be reactive to technological developments and are limited in scope, prohibiting or regulating only specific weapons defined by their design, intent, and characteristics.[40]

However, the use of nanotechnology is already restricted to the extent that it is used to develop or enhance weapons that are prohibited by existing arms control treaties, such as biological weapons,[41] chemical weapons,[42] non-detectable

36 For a detailed analysis of the failed attempt to ban the use of multi-walled carbon nanotubes and silver nanomaterials in the European Union, see, Hitoshi Nasu and Tom Faunce, 'The proposed ban on certain nanomaterials for electrical and electronic equipment in Europe and its global security implications: a search for an alternative regulatory approach', in *European Journal of Law and Technology*, Vol. 2, No. 3, 2011, available at: http://ejlt.org//article/view/79 (last visited 30 October 2012).

37 See, e.g., National Industrial Chemicals Notification and Assessment Scheme (NICNAS), 'Guidance on new chemical requirements for notification of industrial nanomaterials', 2010, available at: http://www.nicnas.gov.au/Current_Issues/Nanotechnology/Guidance%20on%20New%20Chemical%20Requirements%20for%20Notification%20of%20Industrial%20Nanomaterials.pdf (last visited 30 October 2012).

38 Hitoshi Nasu and Tom Faunce, 'Nano-safety or nano-security? Reassessing Europe's nanotechnology regulation in the context of international security law', in *European Journal of Risk Regulation*, Vol. 3, 2012, pp. 416–421.

39 See Jim Whitman, 'The arms control challenges of nanotechnology', in *Contemporary Security Policy*, Vol. 32, No. 1, 2011, pp. 99–115. Cf. J. Altmann, above note 4, pp. 154–176; Sean Howard, 'Nanotechnology and mass destruction: the need for an inner space treaty', in *Disarmament Diplomacy*, Vol. 65, 2002, available at: http://www.acronym.org.uk/dd/dd65/65op1.htm (last visited 30 October 2012).

40 Frits Kalshoven, 'The Conventional Weapons Convention: underlying legal principles', in *International Review of the Red Cross*, Vol. 30, No. 279, 1990, p. 518; Timothy L. H. McCormack, 'A non-liquet on nuclear weapons – the ICJ avoids the application of general principles of international humanitarian law', in *International Review of the Red Cross*, No. 316, 1997, p. 90.

41 Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, 10 April 1972, 1015 UNTS 163 (entered into force 26 March 1975).

42 Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, 13 January 1993, 1974 UNTS 45 (entered into force 29 April 1997).

fragments,[43] blinding laser weapons,[44] anti-personnel mines,[45] explosive remnants of war,[46] and, most recently, cluster munitions.[47] Nanotechnology, if used as an enabling technology for weapons development in these areas, would be regulated by the relevant treaty. Nanotechnology, for example, can produce lasers far more powerful than those previously known.[48] The ability of nanotechnology to design and manipulate molecules with specific properties could lead to bio/chemical agents capable of causing defined hostile results ranging from temporary incapacitation to death, or multilayered biochemical carriers that could easily control the spread of bio/chemical agents.[49]

General principles of international humanitarian law, conversely, tend to refer to the effects produced by the use of means or methods of warfare.[50] The general principle that 'the right of belligerents to adopt means of warfare is not unlimited' has been codified in international humanitarian law instruments.[51] This general principle and other rules of international humanitarian law must be read in light of the Martens Clause.[52] Although 'principles of humanity' and 'dictates of public conscience' alone may provide no firm legal basis to prohibit the use

43 Protocol (I) on Non-Detectable Fragments to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects, 10 October 1980, 1342 UNTS 137 (entered into force 2 December 1983).

44 Protocol (IV) on Blinding Laser Weapons to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have indiscriminate Effects, 13 October 1995, 1380 UNTS 370 (entered into force 30 July 1998).

45 Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction, 4 December 1997, 2056 UNTS 211 (entered into force 1 March 1999).

46 Protocol (V) on Explosive Remnants of War to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects, 28 November 2003, 2399 UNTS 100 (entered into force 12 November 2006).

47 Convention on Cluster Munitions, 3 December 2008 (entered into force 1 August 2010).

48 Geoffrey Duxbury *et al.*, 'Quantum cascade semiconductor infrared and far-infrared lasers: from trace gas sensing to non-linear optics', in *Chemical Society Reviews*, Vol. 34, No. 11, 2005, pp. 921–934.

49 Juan Pablo Pardo-Guerra and Francisco Aguayo, 'Nanotechnology and the international regime on chemical and biological weapons', in *Nanotechnology Law and Business*, Vol. 2, No. 1, 2005, pp. 58–59; Margaret E. Kosal, 'The security implications of nanotechnology', in *Bulletin of Atomic Scientists*, Vol. 66, July/August 2010, pp. 58–69. Cf. Robert D. Pinson, 'Is nanotechnology prohibited by the Biological and Chemical Weapons Conventions?', in *Berkeley Journal of International Law*, Vol. 22, 2004, p. 298.

50 Christopher Greenwood, 'The law of weaponry at the start of the new millennium', in Michael N. Schmitt and Leslie C. Green (eds), *The Law of Armed Conflict: Into the New Millennium*, US Naval War College International Law Studies, Vol. 71, Naval War College, Newport, 1999, p. 192.

51 Regulations Respecting the Laws and Customs of War on Land, CTS, Vol. 205, 1907, p. 277, 18 October 1907 (entered into force 26 January 1910), Article 22, reproduced in Adam Roberts and Richard Guelff, *Documents on the Laws of War*, 3rd edn, Oxford University Press, Oxford, 2000, pp. 73–82 (hereinafter 1907 Hague Regulations); Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, 8 June 1977, 1125 UNTS 3 (entered into force 7 December 1978), Art. 35(1) (hereinafter Additional Protocol I).

52 Declaration Renouncing the Use, in Time of War, of Explosive Projectiles under 400 Grammes Weight, CTS, Vol. 138, 1868–1869, p. 297, 11 December 1868, reproduced in A. Roberts and R. Guelff, above note 51, pp. 54–55 (hereinafter 1968 St Petersburg Declaration); Additional Protocol I, Art. 1(2), which reads: 'In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from dictates of public conscience.'

of particular weapons,[53] the Martens Clause has become especially important as new technologies increasingly affect the development and sophistication of weapons and delivery systems, something which was not envisaged by the drafters of international humanitarian law instruments.[54]

In light of this, the following sections discuss the legal challenges posed by the development of nanotechnology with respect to four basic rules of international humanitarian law: (1) the obligation to ensure the legality of weapons; (2) distinction; (3) proportionality; and (4) precaution.

The legality of weapons[55]

When assessing the legality of weapons at each stage of their development and acquisition, states are required, under Article 36 of Additional Protocol I, to take into consideration the health-related impact of the use of the weapon. Such assessment, equally valid for nanotechnology, must be based on all the relevant scientific evidence.[56] The principle prohibiting the employment of arms, projectiles, or material 'of a nature to cause superfluous injury' (or 'calculated to cause unnecessary suffering'),[57] as well as the principle prohibiting the 'methods or means of warfare which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment',[58] is central to the consideration of legality of nanotechnology-enabled or enhanced weapons under international humanitarian law.[59] For the purpose of this weapons review, superfluous injury or unnecessary suffering is examined only in light of the broad and general circumstances in which the weapon is intended for use, as opposed to a particular use of a weapon which is assessed against the rules of distinction, proportionality, and precaution in the operational context of a particular attack.[60]

53 See, e.g., Christopher Greenwood, 'Historical development and legal basis', in Dieter Fleck (ed.), *Handbook of International Humanitarian Law*, 2nd edn, Oxford University Press, Oxford, 2008, p. 101; Antonio Cassese, 'The Martens Clause: half a loaf or simply pie in the sky?', in *European Journal of International Law*, Vol. 11, 2000, p. 187; Theodor Meron, 'The Martens Clause, principles of humanity, and dictates of public conscience', in *American Journal of International Law*, Vol. 94, 2000, p. 78. Cf. International Court of Justice (ICJ), *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ Reports 1996*, pp. 405–409 (Judge Shahabuddeen dissenting opinion).

54 Stuart Walters Belt, 'Missiles over Kosovo: emergence, *lex lata*, of a customary norm requiring the use of precision munitions in urban areas', in *Naval Law Review*, Vol. 47, 2000, p. 140.

55 For a more detailed analysis of this issue, see Hitoshi Nasu and Tom Faunce, 'Nanotechnology and the international law of weaponry: towards international regulation of nano-weapons', in *Journal of Law, Information and Science*, Vol. 20, 2010, pp. 20, 34–43.

56 See ICRC, 'A guide to the legal review of new weapons, means and methods of warfare: measures to implement Article 36 of Additional Protocol I of 1977', 2006, pp. 18–19, available at: http://www.icrc.org/eng/assets/files/other/icrc_002_0902.pdf (last visited 30 October 2012).

57 Additional Protocol I, Art. 35(2).

58 Additional Protocol I, Art. 35(3).

59 Cf. Antonio Cassese, *The Human Dimension of International Law: Selected Papers*, Oxford University Press, Oxford, 2008, p. 214 (stating that the principle remains a 'significant source of inspiration').

60 See, e.g., Bill Boothby, 'The law of weaponry – is it adequate?', in Michael N. Schmitt and Jelena Pejic (eds), *International Law and Armed Conflict: Exploring the Faultlines, Essays in Honour of Yoram Dinstein*, Martinus Nijhoff, Leiden, 2007, p. 303.

The principle prohibiting superfluous injury or unnecessary suffering was first enunciated in the preamble to the 1868 St Petersburg Declaration,[61] but this general principle was a rhetorical expression of the drafters' inspiration, rather than of their intention to impose legal obligations.[62] It was formally adopted as a binding rule in the subsequent treaties,[63] and since then has attained the status of customary international law.[64] This principle applies universally, irrespective of the distinction between civilian and military targets.[65] The prohibition is now incorporated into the 1998 Rome Statute of the International Criminal Court as a war crime.[66] This principle is of central relevance to the use of nanotechnology in the development of weapons, insofar as those weapons could cause unnecessary suffering.

Yet, exactly which use of nanotechnology in weaponry is deemed illegal depends on the interpretation of what constitutes 'superfluous injury' and 'unnecessary suffering'. One may take a subjective approach by looking at the primary purpose for which the new weapon is designed in order to determine whether it causes injury or suffering disproportionate to its military effectiveness.[67] This dominant view suggests that one must balance the degree of injury or suffering inflicted on the one hand, and the degree of military necessity underlying the choice of particular weapon on the other.[68] The other, more objective approach to 'superfluous injury' or 'unnecessary suffering' under international humanitarian law places greater emphasis on excessive harm inflicted on the victim in relation to the damage necessary to place a combatant *hors de combat* for the duration of combat.[69]

61 It reads that 'the employment of arms which uselessly aggravate the sufferings of disabled men, or render their death inevitable . . . would, therefore, be contrary to the laws of humanity'.

62 F. Kalshoven, above note 40, p. 511.

63 Hague Convention (II) Respecting the Laws and Customs of War on Land, CTS, Vol. 187, 1899, p. 227, 29 July 1899 (entered into force 4 September 1900), Art. 23(e); 1907 Hague Regulations, Art. 23(e). Although the authentic French text remained the same (*maux superflus*), the identical phrase in the two instruments was translated differently. The English translation of the treaty texts is provided in James Brown Scott, *The Hague Conventions and Declarations of 1899 and 1907*, Oxford University Press, New York, 1915, p. 116. Article 35(2) of Additional Protocol I places those two expressions side by side.

64 See, e.g., Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law*, Cambridge University Press, Cambridge, 2005, Vol. 1, pp. 237–244.

65 See *Legality of Nuclear Weapons Advisory Opinion*, above note 53, p. 257, para. 78.

66 See Rome Statute of the International Criminal Court, 17 July 1998, 2187 UNTS 3 (entered into force 1 July 2002), Art. 8(2)(b)(xix) and (xx).

67 This was the view generally held by states during the UN Conference on Certain Conventional Weapons in 1979–1980. See, e.g., W. Hays Parks, 'Conventional weapons and weapons reviews', in *Yearbook of International Humanitarian Law*, Vol. 8, 2005, pp. 76–82; William J. Fenrick, 'The Conventional Weapons Convention: a modest but useful treaty', in *International Review of the Red Cross*, No. 279, 1990, p. 500.

68 Yves Sandoz, Christophe Swinarski and Bruno Zimmerman (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, International Committee of the Red Cross and Martinus Nijhoff Publishers, Geneva, 1987, p. 408, para. 1428 (hereinafter ICRC Commentary). For critical analysis see, e.g., C. Greenwood, above note 50, pp. 195–199; Frits Kalshoven, 'Arms, armaments and international law', in *Recueil des Cours*, Vol. 191, 1985-II, pp. 234–235; Henri Meyrowitz, 'The principle of superfluous injury or unnecessary suffering: from the Declaration of St. Petersburg of 1868 to Additional Protocol I of 1977', in *International Review of the Red Cross*, Vol. 34, No. 299, 1994, pp. 106–109.

69 Rosario Domínguez-Matés, 'New weaponry technologies and international humanitarian law: their consequences on the human being and the environment', in Pablo Antonio Fernández-Sánchez (ed.), *The New Challenges of Humanitarian Law in Armed Conflicts: In Honour of Professor Juan Antonio*

Depending on which approach is taken, the legality of a military application of nanotechnology may well be considered differently. This is particularly so when the application of nanotechnology is designed to enhance penetration capabilities of a weapon, such as thermobaric explosives, to destroy targets inside hardened and deeply buried structures or buildings, yet potentially involving hazardous health and environmental impacts. For example, the deployment of nano-energetic thermobaric explosives could well be justified on the grounds that targeting terrorists or insurgents inside hardened compounds outweighs considerations of severe suffering from the primary blast or thermal damage for combatants or civilians taking a direct part in hostilities.

There is a subtle difference under this international humanitarian law principle between 'injury' and 'suffering'. The former indicates immediate, physical damage, whereas the latter may entail the incidence of permanent damage or disfigurement.[70] This distinction, and emphasis on permanent damage or disfigurement, is of increased significance given that, as is the case with ENMs and ENPs, technological advancement is making it more difficult to scientifically appreciate the full range of damaging effects of a new weapon on the human body by looking only at the weapon's construction.[71] In fact, the idea to extend the meaning of suffering even to harmful effects that ensue after the end of hostilities reportedly influenced the treaty negotiations about blinding laser weapons, particularly the long-term impact of blind veterans on society.[72] An expanded reading of suffering in the application of this principle is one way of casting light on social costs associated with the health and environmental hazards produced by the release of toxic ENMs and ENPs during warfare, which are imposed upon peacebuilding efforts in the aftermath of warfare.[73] Yet, scientific uncertainty surrounding the health and environmental effects of ENMs and ENPs, particularly in relation to the causal link between the weapon and the hazards, makes it a formidable task to prove the suffering.[74] This is due to the difficulties of adequately accounting for combined toxic effects of, and interactions between, different substances.

Insofar as the toxic effects of ENMs and ENPs could extend to the natural environment, including micro-organisms in the soil and water and follow-on effects

Carrillo-Salcedo, Martinus Nijhoff, Leiden, 2005, p. 115; Éric David, *Principes de Droit des Conflits Armés*, 4th edn, Bruylant, Brussels, 2008, pp. 358–361.

70 Michael Bothe, Karl Josef Partsch and Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, Martinus Nijhoff Publishers, The Hague, 1982, p. 196.

71 For a similar view in the context of fragmentation of bullets, see, Robin Coupland, 'Clinical and legal significance of fragmentation of bullets in relation to size of wounds: retrospective analysis', in *British Medical Journal*, Vol. 319, 1999, pp. 403–406.

72 See Burrus M. Carnahan and Marjorie Robertson, 'The Protocol on "blinding laser weapons": a new direction for international humanitarian law', in *American Journal of International Law*, Vol. 90, 1996, p. 485. The same influence can be observed in relation to the treaties on explosive remnants of war, in particular regarding anti-personnel landmines and cluster munitions.

73 Cf. Carl E. Bruch *et al.*, 'Post-conflict peace building and natural resources', in *Yearbook of International Environmental Law*, Vol. 19, 2008, p. 58.

74 Cf. William H. Boothby, *Weapons and the Law of Armed Conflict*, Oxford University Press, Oxford, 2009, p. 364.

on the food chain, the legality of nanotechnology-enabled or enhanced weapons must also be considered in light of Article 35(3) of Additional Protocol I. This provision prohibits the use of 'methods or means of warfare which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment'.[75] This threshold is understood to constitute cumulative requirements and hence impose significant obstacles to ruling any particular attack illegal.[76] Nonetheless, it is debatable whether toxic ENMs and ENPs, released upon impact of nanotechnology-enabled or enhanced weapons (and also arguably as a result of deliberatively targeting nanotechnology-enabled or enhanced objects by conventional kinetic means), have the potential to satisfy this threshold. This is because of the unique characteristics of ENMs and ENPs such as high emission rates,[77] the potential long-range transport through agglomeration or attachment to pre-existing background aerosol particles,[78] and low solubility.[79] Unlike toxic chemical agents, ENMs and ENPs do not dissolve or biodegrade in the environment. Also, unlike biological agents, ENMs and ENPs may travel a long distance without requiring living organisms as carriers for transmission.

Unlike the prohibition on superfluous injury or unnecessary suffering, this environmental protection clause is understood as imposing a 'should have known' standard for finding breach without leaving scope for balancing against military necessity or proportionality.[80] It is not clear what level or amount of knowledge or information is required regarding the potential consequences of using nanotechnology-enabled or enhanced weapons, given the currently inconclusive scientific evidence regarding widespread, long-term, and severe environmental hazards posed by the dispersion of ENMs and ENPs. If the health or environmental

75 The ICRC Commentary considers that the term 'natural environment' in the Protocol refers to the 'system of inextricable interrelations between living organisms and their inanimate environment': ICRC Commentary, above note 68, para.1451.

76 See ICRC Commentary, above note 68, para. 1457; M. Bothe, K. J. Partsch and W. A. Solf, above note 70, pp. 347–348. This is contrasted with the Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques, 10 December 1976, 1108 UNTS 152 (entered into force 5 October 1978) (ENMOD Convention), which uses a disjunctive formula ('widespread, long-lasting or severe'). This Convention does not prohibit or regulate the use of nanotechnology unless it is specifically used to manipulate the environment for hostile purposes. For an analysis of this Convention, see, e.g., Jozef Goldblat, 'The Environmental Modification Convention of 1977: an analysis', in Arthur H. Westing, (ed.), *Environmental Warfare: A Technical, Legal and Policy Appraisal*, Taylor & Francis, London, 1984, p. 53.

77 See Denis Bémer *et al.*, 'Ultrafine particles emitted by flame and electric arc guns for thermal spraying of metals', in *Annals of Occupational Hygiene*, Vol. 54, No. 6, 2010, pp. 607–614.

78 See Martin Seipenbusch and Gerhard Kasper, *Recommendations to the European Commission – Transport of Nanoparticles in the Workplace Environment and Its Effects on the Size Spectrum*, Nanotransport-Project, 30 April 2008, available at: http://research.dnv.com/nanotransport/NANOTRANSPORT download/Recommendations-final-EC.pdf (last visited 30 October 2012); US EPA, above note 6, p. 33. Cf. Lan Ma-Hock *et al.*, 'Generation and characterization of test atmospheres with nanomaterials', in *Inhalation Toxicology*, Vol. 19, No. 10, 2007, pp. 833–848 (observing that as for many substances, agglomeration effects limited nanoparticle exposure).

79 See V. Stone, H. Johnston and M. J. Clift, 'Air pollution, ultrafine and nanoparticle toxicology: cellular and molecular interactions', in *IEEE Trans Nanobioscience*, Vol. 6, No. 4, 2007, pp. 331–340 (showing that ultrafine particles are found more toxic and inflammogenic than fine particles due to low solubility).

80 Michael N. Schmitt, 'Green war: an assessment of the environmental law of international armed conflict', in *Yale Journal of International Law*, Vol. 22, 1997, pp. 72–73.

concerns fail to reach this threshold, then they would have to be considered in light of whether the prohibition on superfluous injury or unnecessary suffering extends to accommodate those concerns as 'suffering'.

Distinction

The cardinal point in the principle of distinction is that combatants are clearly distinguishable from civilians, who are not to be directly targeted.[81] This principle is enunciated in Article 48 of Additional Protocol I, which reads: '[t]he Parties to the conflict shall at all times distinguish between the civilian population and combatants ... and accordingly shall direct their operations only against military objectives.'[82] This principle imposes two inextricably connected obligations: it requires states to direct their military attacks only against combatants, on the one hand; and, in order to enable states to comply with the first obligation, it requires them to distinguish combatants from civilians by means of, inter alia, 'a characteristic piece of clothing which is visible'.[83]

Stealth technology has already been introduced for military aircraft to reduce the visibility and the probability of detection by radar, infrared, or other probe beams.[84] However, nanofabrication technology has the potential to enhance this stealth technology further by enabling optical camouflage (also often called adaptive camouflage).[85] Using optical camouflage in all of three light spectrums – visible light, night-vision spectrum, and thermal/infrared spectrum – to cloak soldiers and their equipment will enable complete invisibility, undetectable by any traditional means of warfare until a new detection technology is developed.[86] Camouflaging is a typical example of traditional military tactics of deception permitted as ruses of warfare.[87] It is not prohibited insofar as no rule of international humanitarian law is infringed and it cannot be considered a perfidious act insofar as it does not invite the confidence of the enemy with respect to protection under international humanitarian law.[88]

81 The principle of distinction has been recognized as customary international law. See, e.g., *Legality of Nuclear Weapons Advisory Opinion*, above note 53, p. 257, para. 78; J.-M. Henckaerts and L. Doswald-Beck, above note 64, Vol. 1, Rule 1.

82 Additional Protocol I, Art. 48. See also, 1907 Hague Regulations, Art. 1(2) (requiring combatants '[t]o have a fixed distinctive emblem *recognizable* at a distance' (emphasis added)); Geneva Convention Relative to the Treatment of Prisoners of War of August 12, 1949, 12 August 1949, 75 UNTS 135 (entered into force 21 October 1950), Art. 4(A)(2)(b) ('having a fixed distinctive sign *recognizable* at a distance' (emphasis added)).

83 ICRC Commentary, above note 68, p. 528, para. 1693.

84 See generally, Tae-Woo Lee, *Military Technologies of the World*, Praeger Security International, Westport, 2009, Vol. 1, pp. 178–180.

85 See A. Di Falco *et al.*, above note 19.

86 See H. Shi *et al.*, above note 20, p. 211103-1 (suggesting that the low refractive index of carbon nanotubes can absorb light and cloak an object against a black background).

87 See generally, UK Ministry of Defence, *The Manual of the Law of Armed Conflict*, Oxford University Press, Oxford, 2004, p. 64; Leslie C. Green, *The Contemporary Law of Armed Conflict*, 2nd edn, Manchester University Press, Manchester, 2000, pp. 146–147, 186–187.

88 Additional Protocol I, Art. 37(1) and (2).

Yet, in situations where cloaked combatants launch attacks from within a civilian-populated area, the only way the adverse party can counter-attack is to fire in the direction the attacks came from without being able to identify or distinguish combatants from civilians. The adverse party is thus prevented from complying with the principle of distinction. Similar difficulties have arisen in situations where combatants are firing from civilian buildings; however, enhanced optical camouflaging effectively deprives the adverse party of any chance to detect lawful military targets. This may well raise a significant issue challenging the application of the principle of distinction. Thus cloaking devices must be used with necessary precautions against endangering civilians.[89]

The application of nanotechnology to facilities for complete or partial military use, on the other hand, does not challenge the application of the principle of distinction. Attacks must be directed against legitimate military objectives, which are defined by Article 52(2) of Additional Protocol I, as objects 'which by their nature, location, purpose, or use make an effective contribution to military action and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offer a definite military advantage'. Therefore, any facility, installation, or building, no matter how or whether ENMs and ENPs are used, is not immune from becoming a legitimate military target.

Special protection is accorded to dams, dykes, and nuclear electricity-generating stations under Article 56 of Additional Protocol I because of concern about the release of dangerous forces and consequent severe damage to the civilian population as a result of an attack against those works and installations.[90] Yet, alternative electricity-generating stations, such as nanotechnology-enhanced solar power plants,[91] do not fall under this category of specially protected objects. Even if targeting nanotechnology-enhanced solar power plants may result in the release of toxic ENMs and ENPs into the environment and human bodies, the environmental and health risks do not make those plants immune from direct military attacks. Rather, as will be discussed below, those effects are more likely to be relevant to the principles of proportionality and precaution.

Thus, no electricity-generating station, whether nanotechnology enhanced or not, is currently protected from direct attacks under international humanitarian law. It is arguable that, in the future, attacks against nanotechnology-enhanced power plants could result in the release of dangerous forces, prompting a call to amend Article 56 of Additional Protocol I to expand the scope of its legal protection. Alternatively, society may move to more decentralized electricity generation relying on solar panels in each household. In that case, the mere possibility that electric

89 Additional Protocol I, Art. 57.

90 Although it refers generally to 'works and installations containing dangerous forces', the term 'namely' and the intention of the parties during the treaty negotiations make it clear that protected objects are only those listed in the provision. See ICRC Commentary, above note 68, pp. 668–669, paras. 2146–2150; M. Bothe, K. J. Partsch and W. A. Solf, above note 70, p. 354.

91 As noted above, engineered metal nanomaterials are widely seen as having a great potential to enhance the capacity and efficiency of solar power plants. See above note 30 and accompanying text.

power generated from each household is used for military purposes would not necessarily make civilian houses legitimate military objectives.[92]

Proportionality

The principle of proportionality is widely recognized as a rule of customary international law regulating the conduct of warfare both in international and non-international armed conflicts.[93] Although the term 'proportionality' does not appear in the text of Additional Protocol I,[94] the gist of the principle is reflected in Article 51(5)(b) as an example of indiscriminate attack and also in Article 57(2)(a)(iii) as one of the precautions to be taken, prohibiting 'an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated'. The inherent subjectivity in assessing excessiveness while balancing two different values – anticipated military advantage and expected incidental losses – has been a subject of controversy and even criticism of the practicality of this principle.[95]

Relevant to the implications of nanotechnology is the question as to what extent the 'effect' of attacks must be taken into account in the proportionality calculus, given that the potential health and environmental effects of ENMs and ENPs are the primary concerns about the use of nanotechnology among regulators around the world.[96] The larger the radius of incidental civilian losses is drawn, the more difficult it may become to justify the damage on proportionality grounds. Indirect costs and long-term effects (sometimes called reverberating effects) of a military attack tend to be ignored in the proportionality calculus, as the indirect effects are less visible than direct damage and more difficult to ascertain.[97] However, to the extent that the principle of proportionality is based on the idea of humanity and is influenced by the development of human rights norms,[98] a greater awareness of the indirect and long-term impacts of military attacks may well challenge the validity of traditional practice. Thus, Henry Shu and David Wippman, for example, consider that the loss of a civilian function as a result of destroying a dual-use facility (such as electricity-generating plant) should not be discounted from

92 See James W. Crawford, 'The law of noncombatant immunity and the targeting of national electrical power systems', in *Fletcher Forum of World Affairs*, Summer/Fall 1997, p. 105.
93 See, e.g., J.-M. Henckaerts and L. Doswald-Beck, above note 64, Vol. 1, Rule 14.
94 For a detailed account as to why the reference to proportionality was avoided, see Lt Col. William J. Fenrick, 'The rule of proportionality and Protocol I in Conventional Warfare', in *Military Law Review*, Vol. 98, 1982, pp. 102–106; Frits Kalshoven, 'Reaffirmation and development of international humanitarian law applicable in armed conflicts: the diplomatic conference, Geneva, 1974–1977, Part II', in *Netherlands Yearbook of International Law*, Vol. 9, 1978, p. 117.
95 The literature on this subject is voluminous. See especially, Judith Gardam, *Necessity, Proportionality and the Use of Force by States*, Cambridge University Press, Cambridge, 2004, pp. 98–121.
96 See literature cited above note 8.
97 See, e.g., Christopher Greenwood, 'Customary international law and the First Geneva Protocol of 1977 in the Gulf Conflict', in Peter Rowe (ed.), *The Gulf War 1990–91 in International and English Law*, Routledge, London, 1993, p. 79.
98 See Theodor Meron, *The Humanization of International Law*, Martinus Nijhoff, Leiden, 2006, p. 67.

the proportionality calculus merely because the object is a military objective.[99] More relevantly, considering the implications of recent technological improvements, Michael Schmitt suggests that humanitarian attention may well centre on reverberating effects or derivative consequences, 'now that the means exist to limit dramatically direct collateral damage and incidental injury that we are being sensitized to reverberation'.[100]

Environmental concerns are already acknowledged in a general principle of proportionality. The International Court of Justice (ICJ) observed in its advisory opinion on *Legality of the Threat or Use of Nuclear Weapons* that '[s]tates must take environmental considerations into account when assessing what is necessary and proportionate in the pursuit of legitimate military objectives'.[101] Yet, the extent to which states are required to take environmental considerations into account is far from clear. If the principle of proportionality is read in conjunction with Article 55(1) of Additional Protocol I, relevant considerations are narrowly confined to 'widespread, long-term and severe damage to the natural environment'. Unlike the prohibition under Article 35(3) of Additional Protocol I, environmental considerations referred to in Article 55(1) impose only a duty of care and are focused on the health and survival of the population.[102] This suggests that even if nanotechnology is not involved in the methods or means of warfare employed, commanders are under a duty of care not to cause widespread, long-term, and severe environmental damage that threatens the health or survival of the population when targeting nanotechnology-enabled or enhanced facilities, whether they are legitimate military objectives or not.

Here, the consideration of environmental effects in the context of Article 55(1) of Additional Protocol I is subject to two qualifications. First, commanders are required to take into account widespread, long-term, and severe environmental damage that may be expected to jeopardize the survival of the population or seriously prejudice health by causing, for example, congenital defects, degenerations, or deformities.[103] Therefore, one needs to speculate: (i) whether the attack is likely to involve destruction of nanotechnology-enabled or enhanced facilities; (ii) whether ENMs and ENPs released upon impact might cause widespread, long-term, and severe environmental damage; and (iii) how human bodies and genes are affected by contact with those substances. Yet, the process of transformation, agglomeration, and fusion with larger substances cause tremendous

99 Henry Shue and David Wippman, 'Limiting attacks on dual-use facilities performing indispensable civilian functions', in *Cornell International Law Journal*, Vol. 35, 2002, pp. 565, 573–579.

100 Michael N. Schmitt, 'The principle of discrimination in 21st century warfare', in *Yale Human Rights & Development Law Journal*, Vol. 2, 1999, p. 168.

101 *Legality of Nuclear Weapons Advisory Opinion*, above note 53, p. 242, para. 30.

102 The provision, in full text, reads: '*Care shall be taken* in warfare to protect the natural environment against widespread, long-term and severe damage. This protection includes a prohibition of the use of methods or means of warfare which are intended or may be expected to cause such damage to the natural environment and thereby *to prejudice the health or survival of the population*' (emphasis added). For the difference between Article 35(3) and Article 55(1), see, Michael N. Schmitt, 'Humanitarian law and the environment', in *Denver Journal of International Law and Policy*, Vol. 28, 2000, pp. 275–277.

103 ICRC Commentary, above note 68, pp. 663–664, para. 2135.

scientific difficulties for the precise understanding of the nature and extent of health effects.[104] In future conflicts, commanders will have to face 'the fog of science' in battlefields and exercise the duty of care based on the uncertain probability of risk.

Second, the duty of care leaves some latitude for judgement.[105] It is in this context that the principle of proportionality arguably finds its application in relation to environmental collateral damage.[106] This idea is given a clear expression in Article 8(2)(b)(iv) of the 1998 Rome Statute, which provides in its definition of war crimes:

> Intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects or widespread, long-term and severe damage to the natural environment which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated.

Thus, as an element of war crime, environmental damage, to a limited extent, has been incorporated into the proportionality assessment.[107] Yet again, the scientific uncertainty with regard to the full extent and nature of the environmental and health damage caused by the release of and contact with toxic ENMs and ENPs raises challenging questions as to whether the mere availability of scientific evidence is sufficient to constitute 'knowledge' and how the potentially hazardous environmental and health effects are considered 'excessive'. The same questions apply to the proportionality requirement under international humanitarian law, even though the element of knowledge is more loosely expressed.[108]

Due to these two qualifications, therefore, the application of Article 55(1) of Additional Protocol I is of little practical use when regulating the conduct of warfare to restrict or prevent widespread, long-term and severe environmental damage that may be caused by the dispersion of toxic ENMs and ENPs as a result of military attacks. Conversely, Article 51(5)(b) of Additional Protocol I does not require the expected environmental damage to be widespread, long-term, or severe, and therefore arguably allows for a greater scope of incidental loss to accommodate the consideration of potential environmental and health effects of dispersed ENMs and ENPs, though this scope depends on how widely the incidental loss can be interpreted.

104 See, e.g., Fadri Gottschalk and Bernd Nowack, 'The release of engineered nanomaterials to the environment', in *Journal of Environmental Monitoring*, Vol. 13, 2011, pp. 1145–1155; Jayoung Jeong *et al.*, '*In vitro* and *in vivo* toxicity study of nanoparticles', in Saura Sahu and Daniel Casciano (eds), above note 15, pp. 320–324 (pointing out that very few airborne exposure studies have been conducted).

105 ICRC Commentary, above note 68, p. 663, para. 2133.

106 Cf. Michael Bothe *et al.*, 'International law protecting the environment during armed conflict: gaps and opportunities', in *International Review of the Red Cross*, Vol. 92, No. 879, 2010, pp. 577–578.

107 M. N. Schmitt, above note 102, p. 283. A broader incorporation of environmental effects into the proportionality calculus was suggested in ICTY, 'Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia', in *International Legal Materials*, Vol. 39, 2000, pp. 1262–1263, paras. 15–22 (hereinafter ICTY Final Report). See also, Michael Bothe, 'Legal restraints on targeting: protection of civilian population and the changing faces of modern conflicts', in *Israel Yearbook on Human Rights*, Vol. 31, 2002, pp. 44–45.

108 Additional Protocol I, Arts 51(5)(b), 55(1), and 57(2)(a)(iii) (using the expression 'may be expected').

Precaution

Two different obligations of precaution are stipulated in Articles 57 and 58 of Additional Protocol I: precaution in attack and precaution in defence, respectively.[109] It is widely accepted that the obligation to take precautions in planning or deciding upon an attack is a rule of customary international law.[110] To the extent that the wording of Article 57 incorporates the principle of proportionality, the same legal issue will arise as discussed above in relation to the degree to which health and environmental harm caused by the release of toxic ENMs and ENPs upon impact in an armed attack are considered civilian losses. The obligation of precaution raises an additional issue as to what extent indirect or reverberating effects should be foreseeable – in other words, what level or amount of knowledge is required as the basis for taking precautions.

Interestingly, the ICRC's Customary International Humanitarian Law Study understands that the principle of precaution is to be observed even if there is scientific uncertainty as to the effects on the environment of certain military operations.[111] It is debatable to what extent that reading of the 'precautionary principle', which has developed in the field of international environmental law, has been accepted as an interpretation of the obligation to take precautions under international humanitarian law.[112] However, an application of the precautionary principle in the modern world of nanotechnology would pose significant challenges to military operations, insofar as it would require taking all feasible precautions to minimize the release of toxic ENMs and ENPs as a result of armed attacks, even in the absence of scientific certainty as to the actual toxic effects. It may well be unrealistic to expect that a decision be made to halt an attack on the grounds that the potential health and environmental damage is considered excessive in relation to the concrete and direct military advantage anticipated.

This issue also needs to be addressed in the context of precaution in defence. Article 58 of Additional Protocol I requires state parties to take feasible precautions to, among others things, 'protect civilians and civilian objects against the *dangers* resulting from military operations' (emphasis added). While this obligation is arguably considered a rule of customary international law,[113] the reality is that national regulatory authorities in modern society rarely pay heed to the possibility of future warfare and its effects for civilian life.[114] The seriousness of this

109 For a detailed analysis, see Jean-François Quéguiner, 'Precautions under the law governing the conduct of hostilities', in *International Review of the Red Cross*, Vol. 88, No. 864, pp. 793–821.

110 See J.-M. Henckaerts and L. Doswald-Beck, above note 64, Rule 15.

111 *Ibid.*, Rule 44.

112 Cf. M. Bothe *et al.*, above note 106, p. 575; Richard Desgagné, 'The prevention of environmental damage in time of armed conflict: proportionality and precautionary measures', in *Yearbook of International Humanitarian Law*, Vol. 3, 2000, pp. 125–126; Wil D. Verwey, 'Observations of the legal protection of the environment in times of international armed conflict', in *Hague Yearbook of International Law*, Vol. 7, 1994, p. 52.

113 J.-M. Henckaerts and L. Doswald-Beck, above note 64, Rule 22. Cf. W. Hays Parks, 'Air war and the law of war', in *Air Force Law Review*, Vol. 32, 1990, p. 1, at p. 159 (stating that this provision is not obligatory).

114 ICTY Final Report, above note 107, p. 1271, para. 51. See also, Anthony P. V. Rogers, *Law on the Battlefield*, 2nd edn, Manchester University Press, Manchester, 2004, pp. 120–126.

oversight was illustrated by the increased number of cancer-related deaths in the aftermath of the 9/11 terrorist attacks in New York due to the exposure to toxic dust released from the collapsed buildings.[115] With the impending threat of health and environmental hazards potentially resulting from the release of toxic ENMs and ENPs during warfare, a greater recognition of the obligation to take precautions to protect civilians from the effects of armed attacks arguably has the potential to encourage and facilitate more comprehensive nanotechnology regulation encompassing the prevention and control of exposure to toxic ENMs and ENPs.

Conclusion

Nanotechnology may well be seen as of little concern for the implementation of international humanitarian law in modern warfare, particularly if direct civilian casualties are reduced by the introduction of more sophisticated, precise, and efficient weapons and delivery systems enabled or enhanced by nanotechnology. One need only recall the traditionally held view that the legitimate objective in warfare is to weaken enemy forces by disabling the greatest possible number of combatants.[116] However, the focus of modern warfare has been shifting more towards precision-focused, effects-based military operations, which places an emphasis on achieving certain results rather than the absolute destruction of enemy forces.[117] This shift of military doctrine arguably underlines a greater need to reconsider how and to what extent the potential hazardous effects of ENMs and ENPs on health and the environment should or should not be taken into account when applying basic rules of international humanitarian law.

By examining this question, this article has identified three areas of concern for the application of international humanitarian law that arise from widespread use of nanotechnology. First, scientific uncertainty surrounding the health and environmental impacts of ENMs and ENPs raises an issue concerning the level or amount of knowledge required when considering the legality of a weapon, assessing the excessiveness of an attack, and taking precautions during targeting decision-making. Second, there is no clear guidance as to how widely health and environmental effects resulting from armed attacks must be taken into account, except when the effects are intended, or may be expected, to be widespread, long-term, and severe. This is because of the unsettled debate over the extent to which indirect, long-term impacts should be taken into account when considering what

115 See, World Trade Center Health Program: Addition of Certain Types of Cancer to the List of WTC-Related Health Conditions, US Federal Register, Vol. 77, No. 177, 2012, pp. 56138–56168.

116 See, Preamble to the 1868 St Petersburg Declaration, above note 52.

117 See, e.g., Tomislav Z. Ruby, 'Effects-based operations: more important than ever', in *Parameters*, Vol. 38, No. 3, 2008, p. 26; Edward A. Smith, Jr., 'Effects-based operations', in *Security Challenges*, Vol. 2, No. 1, 2006, p. 43; Elinor C. Sloan, *The Revolution in Military Affairs: Implication for Canada and NATO*, McGill-Queen's University Press, 2002, p. 15; David A. Deptula, *Effects-Based Operations: Change in the Nature of Warfare*, Aerospace Education Foundation, Arlington, 2001, pp. 21–22.

constitutes superfluous injury or unnecessary suffering and also when assessing the excessiveness of an attack. Third, the principle of distinction and the obligation to take precautions will become more difficult to sustain unless the significance of more comprehensive nanotechnology regulation envisaging wartime situations is recognized by national regulatory authorities.

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

Conflict without casualties . . . a note of caution: non-lethal weapons and international humanitarian law

Eve Massingham*

Eve Massingham is an international humanitarian law officer with the Australian Red Cross. She has completed studies in law, international law, and international development.

Abstract

In the last decade considerable expense has been invested in non-lethal weapons development programmes, including by the United States military and other members of the North Atlantic Treaty Organization and members of the European Working Group Non-Lethal Weapons. This paper acknowledges the potential suitability of non-lethal weapons for specific situations arising on the battlefield, but cautions against those who advocate for any weakening of existing international humanitarian law frameworks to provide for greater employment of non-lethal technologies.

Key words: non-lethal weapons, distinction, proportionality, precaution.

The promise of modern international humanitarian law is that those who are *hors de combat* will be protected, respected, and cared for in times of armed conflict. Despite the actions of some, whose blatant disregard for the law and humanity is

* This paper was originally delivered at the Australian and New Zealand Society of International Law's annual conference in Canberra in June 2011. The views expressed in this article reflect the author's opinions and not necessarily those of the Australian Red Cross.
All the Internet references were accessed in January 2012, unless otherwise stated.

doi:10.1017/S1816383112000720

unable to be prevented, through education and increasingly through enforcement, progress continues to be made towards delivering on this promise. That said, it is certainly acknowledged that the modern day battlefield poses many challenges for international humanitarian law. A growing appetite for the development of non-lethal weapon technologies with war-fighting application is the source of one of these challenges. Fidler notes that this kind of '[r]apid technological change will continue to stress international law on the development and use of weaponry, but in ways more politically charged, legally complicated and ethically challenging than the application of international humanitarian law in the past to technologies specifically designed to kill and destroy'.[1]

Non-lethal weapons are those weapons that are designed to incapacitate rather than to kill. The North Atlantic Treaty Organization (NATO) defines non-lethal weapons as those 'weapons which are explicitly designed and developed to incapacitate or repel personnel, with a low probability of fatality or permanent injury, or to disable equipment, with minimum undesired damage or impact on the environment'.[2] Most definitions contain similar elements with a focus on incapacitation rather than elimination. There is a range of non-lethal weapons technologies with differing counter-personnel, counter-material and counter-capability applications. The weapons use a variety of different deployment methodologies including using kinetic, acoustic, directed energies, and/or a combination of these. For example, the Directed Energy Active Denial System fires a 95 GHz-2 millimetre-wave directed energy that rapidly heats a person's skin to achieve a pain threshold without burning the skin.[3] More traditional methods include anti-riot water cannons, some models of which can knock a person down from around 90 metres. These cannons can also be laced with dyes or tear gas. Net launchers, which are a non-lethal way to restrain and control a fleeing or aggressive suspect, are another type of non-lethal weapon. The net can be deployed by a hand-held launcher and is therefore small enough to be used while in pursuit of a fleeing suspect. There is also a counter-small vehicle application for these netting devices.[4] There are a variety of publications that provide considerable technical detail about these weapons.[5] This article does not attempt to discuss them with any technical expertise.

Despite their innocuous name, the potential for these weapons to in fact be lethal is widely noted. The use in October 2002 by Russian security forces of an

1 David Fidler, 'The meaning of Moscow: "non-lethal" weapons and international law in the early 21st century', in *International Review of the Red Cross*, Vol. 87, No. 859, 2005, p. 552.

2 NATO Policy on Non-lethal weapons, available at: http://www.nato.int/docu/pr/1999/p991013e.htm.

3 'Vehicle-Mounted Active Denial System (V-MADS)', in *Globalsecurity*, available at: http://www.globalsecurity.org/military/systems/ground/v-mads.htm.

4 US Department of Defense Non-Lethal Weapons Program, 'M2 Vehicle Lightweight Arresting Device Net', available at: http://jnlwp.defense.gov/current/VLAD.html.

5 See further, Nick Lewer and Neil Davison, 'Non-lethal technologies – an overview', in *Disarmament Forum*, Vol. 1, 2005, pp. 37–51; D. Fidler, 'Meaning of Moscow', above note 1, p. 528; US Department of Defence Joint Non-Lethal Weapons Program website, available at: http://jnlwp.defense.gov/index.html; Neil Davison, *Non-Lethal Weapons*, Palgrave MacMillan, Basingstoke, 2009. Davison notes that the JNLWP is putting its hope firmly in directed energy weapons for the future. N. Davison, *ibid.*, p. 103.

'incapacitating' chemical to end the siege of a Moscow theatre by Chechen rebels (which resulted in approximately 130 deaths from approximately 830 hostages) provides one example of this.[6] On a similar note, some observers of heat ray gun technology have noted its potential to cause second- and third-degree burns, and in some cases even death.[7] 'Non-lethal is a relative term. All weapons . . . create some primary or secondary risk of death or permanent injury.'[8] And of course, with any weapon system there is the potential for abuse.

This article outlines existing legal frameworks that regulate the use of non-lethal weapons in armed conflict – both under the general rules of international humanitarian law and under specific weapons law regimes – before turning to explore the changing legal frameworks and the challenges non-lethal weapons technologies pose to the fundamental principles of international humanitarian law. The law enforcement and policing paradigm is also discussed. The article identifies that there may be some situations where the availability of a non-lethal weapon provides a lawful choice of weapon to a commander, but identifies that even in these situations non-lethal weapons may not be the most appropriate weapons to employ. Finally, the article discusses whether there is an obligation to use a non-lethal weapon in circumstances where it would be available and expected to achieve the military objective. In seeking to establish a balance between military necessity and humanity, the article aims to issue a caution against proposals that may result in any weakening of the fundamental principles of international humanitarian law through the use of non-lethal weapons.

General obligations regarding the use of weapons under international humanitarian law

The Geneva Conventions of 1949 and their Additional Protocols of 1977 are the central documents of international humanitarian law and embody the fundamental principles of international humanitarian law. These documents do not make specific reference to particular weapons, so as to permit or prohibit their use, but rather, through prescribing the principles of distinction, proportionality, and precaution, they establish the means and methods of warfare that can be lawfully employed in armed conflict.

The principle of distinction between military and civilian objects forms the cornerstone of international humanitarian law. Clearly articulated by Article 48 of Additional Protocol I, the principle provides that:

6 See, for example, N. Davison, above note 5, Chapter 1. See also, European Working Group on Non-Lethal Weapons Information Leaflet, above note 39; and D. Fidler, above note 1.
7 Ed Cumming, 'The Active Denial System; The weapon that's a hot topic', in *The Telegraph*, 20 July 2010, available at: http://www.telegraph.co.uk/science/7900117/The-Active-Denial-System-the-weapon-thats-a-hot-topic.html.
8 N. Davidson, above note 5, p. 1.

> In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.

It is widely agreed that this principle has been incorporated into customary international humanitarian law as a norm applicable in both international and non-international armed conflicts.[9]

The principle of proportionality notes that it is prohibited to launch an attack that may be expected to cause incidental loss of civilian life, injury to civilians, or damage to civilian property that would be excessive in relation to the concrete and direct military advantage anticipated.[10] Again, this principle is reflected in customary international humanitarian law for both international and non-international armed conflict.[11] Therefore, while targeting civilians is prohibited, causing injury to civilians or damage to civilian objects is not necessarily unlawful.

The principle of precaution provides that constant care must be taken to spare the civilian population, civilians, and civilian objects. Thus, each party to the conflict must do everything feasible to verify that targets are military objectives, take all feasible precautions in the choice of means and methods of warfare, and cancel or suspend an attack if it becomes apparent that the target is not a military objective or that the attack would violate the principle of distinction or proportionality, or both.[12] The parties must also give advance warning unless circumstances do not permit. In case of doubt about an individual's status as civilian or combatant, or about the nature, purpose, or use of an ordinarily civilian object, the presumption is in favour of that person or object being civilian.[13]

Military personnel and objectives

The rules of international humanitarian law allow the targeting of military personnel and military supplies, transport, and infrastructure (collectively hereinafter military objectives). However, the means or methods of any such targeting are not unlimited and there are prohibitions on causing unnecessary suffering, and on the employment of methods of warfare that may cause widespread, long-term, and severe damage to the natural environment.[14] Some non-lethal weapons, such as blinding laser weapons, have already been assessed by the international community as causing unnecessary suffering. However, if the weapon is not otherwise

9 Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law, Vol. 1: Rules*, ICRC and Cambridge University Press, Geneva, 2005 (hereafter 'ICRC Customary Law Study'), Rule 1, p. 3.
10 API, Arts 51(5)(b) and 57(2)(a)(iii).
11 ICRC Customary Law Study, above note 9, Rule 14.
12 API, Art. 57; ICRC Customary Law Study, above note 9, Rules 15 to 21, pp. 51–67.
13 API, Arts 50 and 52(3).
14 Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflict (Protocol I), 8 June 1977 (hereinafter API), Art. 35.

prohibited by international law and can meet the threshold tests for lawful use in a particular targeting instance – that is, that it is capable of being directed solely against military targets and in circumstances where any incidental civilian loss will not be excessive in relation to the concrete and direct military advantage anticipated – then there is no reason why a non-lethal weapon should not be potentially suitable for deployment in that instance.

From a practical perspective however, there are some additional considerations that military commanders would no doubt want to take into account when selecting a non-lethal weapon to neutralize a military objective. One of these considerations is the actions required to be undertaken by military personnel consequent to causing incapacitation. Under the laws of war, when a person becomes – through injury, incapacitation, or surrender – a person *hors de combat*, obligations flow to the military unit, under whose protection that individual falls, to ensure their care and protection in all circumstances.[15] Non-lethal weapon technology leads to questions such as: how do you recognize that an incapacitated opponent is *hors de combat*; and how would an incapacitated opponent signal the intention to surrender? These questions may be much more difficult to answer than when an opponent is injured by more traditional means. For example, if a tranquilizing weapon is used against an opponent, their incapacitation may not be immediately apparent to others. A tranquilized enemy is *hors de combat*. A sleeping enemy is fair game. Consequently, it may not always be in a military commander's interest to employ a non-lethal weapon where a lethal weapon would comply with international humanitarian law. The availability of non-lethal weapons therefore simply adds to the choice of weapons that are available to a commander. Given the circumstances prevailing at the time, the non-lethal weapon may or may not be an appropriate and lawful weapon for employment in neutralizing an enemy military objective.

Many non-lethal technologies that operate outside the ambit of traditional weapons functions are clearly being employed in such a way as to minimize the number of unnecessary casualties of warfare. One example of this development is the use of acoustic hailing devices with language translation capabilities which allow troops to communicate with a potential enemy at distance – thus facilitating compliance with the principle of distinction – and seek to avoid the use of force if in fact the individual(s) is not hostile.[16] However, while the acoustic hailing device and other similar developments may meet a military commander's definition of a weapon (in that they enable the possibility of incapacitating the enemy when they are used as non-lethal devices capable of releasing a sound pressure that a human cannot stand without hearing protection, or even without suffering hearing loss) these valuable devices seem fairly innocuous in comparison to some of the more alarming developments in non-lethal technologies being developed for battlefield

15 Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949 (hereinafter GCI), Art. 12.

16 Cpl Jahn R. Kuiper, 'Non-lethal weapon developments translates to safe civilians, Marines', in *Marine Corps Base Quantico*, available at: http://www.quantico.usmc.mil/Sentry/StoryView.aspx?SID=5380.

use. Included in the latter category are weapons that appear only to have personnel dispersion application and which, therefore, seem to have limited application in a war-fighting context. The only conceivable use for such weapons is crowd control. Indeed, comments of this nature have been made about the Active Denial System, which was deployed in Afghanistan by the United States Department of Defense but later recalled and never actually used operationally (reasons for the recall have not been given).[17]

Civilians and civilian objects

The principle of distinction requires that at all times military operations be directed only against military objectives. Nothing in international law or state practice would suggest that in the context of an armed conflict (the policing context will be contrasted briefly below) this prohibition on directing attacks against civilians is limited to attacks of a lethal nature. Indeed, provisions of Additional Protocol I and, to a more limited degree, Additional Protocol II make it clear that impacting the civilian population in any way not required by military necessity is prohibited.[18] It is clear then that the non-lethal nature of a weapon does not alter the legality of its use in direct attacks against civilians or civilian objects, as international humanitarian law prohibits direct attacks against these persons and objects by any form of weapon.

However, as discussed above, the principle of proportionality notes that it is prohibited to launch an attack that may be expected to cause incidental loss of civilian life, injury to civilians, or damage to civilian property that would be excessive in relation to the concrete and direct military advantage anticipated. Therefore, while targeting civilians is prohibited, injury to civilians or damage to civilian objects is not necessarily unlawful. Actions that impact on the civilian population or civilian objects are in fact lawful where such impacts are not excessive in relation to the concrete and direct military advantage anticipated. Most military commanders – whether for reasons of humanity, professionalism, economy of effort and resources, or winning hearts and minds – will simply aim to neutralize the enemy and cause the least possible damage to the civilian population in doing so. It is easy to see how the proportionality equation could be swayed in the minds of commanders in favour of an attack by virtue of the non-lethal nature of the effects (which may be viewed as therefore less significant). As Mayer points out, this is particularly the case when 'using [non-lethal weapons] against non-combatants may, in some cases, actually save the non-combatants' lives'.[19] However, this approach does not take into account the unknown elements of non-lethal weapons use. These include the possibility of the effect of the weapon being lethal to a

17 E. Cumming, above note 7.

18 See, for example, API, Part IV, Section I; Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977 (hereafter APII), part IV.

19 Chris Mayer, 'Nonlethal weapons and noncombatant immunity: is it permissible to target noncombatants?', in *Journal of Military Ethics*, Vol. 6, No. 3, 2007, pp. 221.

particular individual, or group of individuals, or the weapon inflicting long-term health consequences on those they are used against.

There is therefore a very real possibility that the availability of a non-lethal weapon as an option for commanders may contribute to a weakening of this prohibition on targeting civilians. This is perhaps particularly so on the battlefield where non-state actors, militia, 'terrorists', and private military and security companies pose a threat to the fundamental principle of distinction by blurring the lines between combatant and civilian. The notion of combatant privilege – the right to kill and its corresponding duties, including the duty to protect and respect those *hors de combat* – is absolutely central to the effectiveness of international humanitarian law. On a battlefield where it is increasingly more and more difficult to distinguish between combatants and non-combatants, to identify threats, or to determine if a civilian has lost his or her protection under international humanitarian law by virtue of his or her 'direct participation in hostilities',[20] one can appreciate the temptation to 'incapacitate now' to allow asking questions later, rather than employing the more traditional 'shoot now' approach, which is less likely to offer opportunities for interrogation after the fact.

However, while this blurring of the lines brings new challenges, it does not change the fundamental nature of the presumption against combatant status – that is, the principle of precaution under international humanitarian law (in effect, 'when in doubt, don't shoot'). Work in this field should continue to further strengthen protection for civilians in times of conflict rather than erode it. This is an important international agenda, and one that the International Red Cross and Red Crescent Movement continues to champion.

Weapons law treaties

Some non-lethal weapons technologies are dealt with by existing international humanitarian law treaties and other legal frameworks. Some representative prohibitions include the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (BWC)[21] and the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (CWC).[22] The latter provides for the prohibition of any chemical that, through its chemical action on life processes, can cause death, temporary incapacitation, or permanent harm to humans or animals. The protocols to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional

20 GCs, Art. 3 common; API, Art. 51(3); ICRC Customary Law Study, above note 9, Rule 6; Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, ICRC, Geneva, 2009.

21 Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, better known as the Biological Weapons Convention (BWC), opened for signature on 10 April 1972.

22 Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (CWC), opened for signature on 13 January 1993.

Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects[23] also deal with a number of potential non-lethal weapons technologies, such as non-detectable fragments, mines, and booby traps and blinding laser weapons.

Review obligations under Article 36 of Additional Protocol I

Although rules pertaining to specific weapons technologies are left to other documents, the need for the law to accommodate developments in technology was clearly foreseen by the drafters of the Additional Protocols of 1977. Article 36 of Protocol I provides that in the development of new weapons, means, or methods of warfare, High Contracting Parties are under an obligation to consider whether their employment would violate international humanitarian law. The idea for the facilitation of compliance with Article 36 was originally that a Committee of States Party be established to consider the legality of the use of new weapons. However, this proposal did not gain the required two-thirds majority and has not come into effect.[24]

Over the years the ICRC has taken a number of measures in an attempt to encourage states to adopt formal systems for compliance with Article 36. The 27th International Conference of the Red Cross and Red Crescent in 1999 and the 28th Conference in 2003 both 'called on states to establish mechanisms and procedures to determine the conformity of weapons with international law'.[25] The 2006 publication, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare*, is designed to assist states to establish weapons review mechanisms.[26]

Lawand notes that:

> The obligation to review the legality of new weapons implies at least two things. First, a state should have in place some form of permanent procedure to that effect, in other words a *standing mechanism* that can be automatically activated at any time that a state is developing or acquiring a new weapon. Second, for the authority responsible for developing or acquiring new weapons such a procedure should be made *mandatory*, by law or by administrative directive. Other than these minimum procedural requirements, it is left to each state to decide what specific form its review mechanism will take.[27]

23 See Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects (with Protocols I, II and III), opened for signature on 10 October 1980.

24 Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Martinus Nijhoff, Geneva, 1987, pp. 422–423.

25 Kathleen Lawand, 'Reviewing the legality of new weapons, mean and methods of warfare', in *International Review of the Red Cross*, Vol. 88, No. 864, December 2006, p. 926.

26 ICRC, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare*, January 2006, available at: http://www.icrc.org/eng/assets/files/other/icrc_002_0902.pdf

27 K. Lawand, above note 25, p. 927.

No doubt Article 36 was drafted with weapons of an increasingly deadly and destructive nature in mind. Nonetheless, there is nothing to suggest that non-lethal weapons technologies are not covered by this provision. However, to date this method of regulation has proved somewhat lacking in effectiveness as only a handful of states have such mechanisms in place.[28] The ICRC seeks, as part of its mandate as the custodian of the Geneva Conventions, to encourage and assist state parties in this process.

Changing legal frameworks

In his 2001 analysis of the future of international humanitarian law and non-lethal weapons, Fidler outlined their future relationship as potentially going one of three ways – using the terms 'radical change', 'selective change', and 'compliance perspective'.[29] The 'radical change' perspective falls at the revolutionary end of the continuum[30] and implicitly challenges the *jus ad bellum/jus in bello* division that is so central to the effectiveness of modern day international humanitarian law. This theory includes the notion that the availability of non-lethal weapons could widen the circumstances in which force can be used in international law. Fidler notes, for example, that this theory could suggest that non-lethal weapons could be used in situations of humanitarian intervention and anticipatory self-defence to make these two concepts more palatable to those who oppose these courses of action. This appears to be a very slippery slope upon which to sit. Little is to be gained by taking such an approach. The prohibition on the use of force in international law is intentionally widely encompassing and, for all its faults, has served humanity well. Conflating *jus ad bellum* and *jus in bello* in this manner can only end in the erosion of *jus in bello*, which would only be to humanity's detriment.

By contrast, the 'selective change perspective advocates that changes in international law may be necessary to allow NLWs [non-lethal weapons] to be used as required for military and humanitarian reasons'.[31] The rationale behind this stems from the idea that these laws were surely never intended to require the killing of persons where a non-lethal option was available.[32] Finally, Fidler's 'compliance perspective' approach says that any tension between international humanitarian law and non-lethal weapon development should be resolved in favour of international humanitarian law.[33]

It is clear that Fidler's 'compliance perspective' is the one that most closely reflects what has occurred in the decade following his work. Indeed, it is not too fanciful to read into the recall of the Active Denial System an appreciation that such technologies have no place on the modern day battlefield because their only

28 ICRC, *A Guide*, above note 26, p. 5.
29 David Fidler, 'Non-lethal weapons and international law: three perspectives on the future', in *Medicine, Conflict and Survival*, Vol. 17, No. 3, 2001, pp. 194–206.
30 *Ibid.*, p. 195.
31 *Ibid.*, p. 199.
32 *Ibid.*, p. 200.
33 *Ibid.*, pp. 198–199.

potential beneficial use could be to disperse a civilian crowd. Such an action would be generally recognized as outside the ambit of lawful actions in armed conflict because combatants have no right to direct their attacks – whether lethal or non-lethal – towards civilians not directly participating in hostilities.[34]

Law enforcement and policing paradigm

It is also worth mentioning the fact that the law enforcement and policing paradigm is confronted with different challenges to those faced by the military in the deployment of non-lethal weapons. Analysis of the use of tasers and Oleoresin Capsicum spray (commonly know as pepper spray) demonstrate that these weapons are often deployed in situations where, prior to their availability, lethal force would never have been used.[35] However, while in a policing context it may be both appropriate and lawful to use non-lethal force against citizens, this is not the case with respect to warfare. As citizens of nations with democratically elected parliaments, many of us in the world have de facto consented to police powers that allow the use of force against citizens for the maintenance of law and order in our societies. Provided such measures do not infringe on any human rights or other applicable laws, the use of such measures is therefore legitimate in many circumstances.

In contrast, it is clear that as citizens of the world we have not consented to the use of force against civilians not directly participating in hostilities in a military context; this is best demonstrated by the strong prohibitions on civilian targeting contained in the universally ratified Geneva Conventions as well as in Additional Protocol I. However, where militaries are effectively exercising police powers (as is often the case, particularly on peacekeeping missions), the line can be difficult to draw. The Australian-led International Force for East Timor (INTERFET), which was authorized pursuant to UN Security Council Resolution 1264 (issued on 15 September 1999) to 'take all necessary measures to restore security in the crisis-ravaged territory of East Timor', over a period of a number of years ran a detention facility in Dili that housed inmates – fewer of whom were detained for reasons pertaining to the conflict were detained because they were disrupters of the peace on Dili's streets. This UN Security Council authorized security mission was, however, very different from traditional war fighting where those persons not taking part in the hostilities are off limits to military personnel. Therefore, it is clear that in some contexts military personnel will be tasked with roles where non-lethal weapons may have very practical application.

34 Although arguably may be permissible, in some circumstances, under the law of occupation.

35 Stephen Coleman, 'Discrimination and non-lethal weapons: issues for the future military', in David Lovell (ed.), *Protecting Civilians during Violent Conflict*, Ashgate, Farnham, 2012, p. 227.

Circumstances where non-lethal weapons provide a good option for commanders

These observations do not imply that non-lethal weapons have no place in armed conflict. Indeed, non-lethal weapons are potentially a suitable choice of weapon by a commander and appropriate for application in circumstances where a lawful attack is known to be likely to cause damage to civilians or civilian infrastructure; that is, an attack on a military objective where any incidental loss of civilian life, injury to civilians, or damage to civilian objects is not excessive in relation to the concrete and direct military advantage anticipated.[36] The use of human shields serves as perhaps the best example of this. While according to international humanitarian law civilians cannot be directly targeted, if surrounding or protecting a legitimate military target – whether intentionally or not – in circumstances where the balancing act of proportionality would allow an attack, their death or injury is considered lawful, provided that sufficient precautionary measures are taken. In such circumstances, an attack that used non-lethal technology, but still had the required counter-material or counter-capability effect to displace or neutralize human shields, would potentially render appropriate the use of non-lethal technology.

Obligation to use

A further issue that has been raised in respect of non-lethal weapons is whether there is an *obligation* to use a non-lethal weapon in circumstances where it would be available and expected to achieve the military objective. Fidler notes that the NATO response to this question is firmly against any such obligation. '[N]either the existence, the presence, nor the potential effect of Non-Lethal Weapons shall constitute an obligation to use Non-Lethal Weapons, or impose a higher standard for, or additional restrictions on, the use of lethal force.'[37] This view is of course not universal. Koplow has argued that the current state of international humanitarian law is 'unlikely to hold', and has predicted a raising of the bar in respect of the threshold for the use of lethal force.[38] The European Working Group Non-Lethal Weapons Information Leaflet notes that non-lethal weapons should be used '[w]hen it is deemed safe to do so and it is believed any life may be saved'.[39] The failure to add to this statement the qualifier 'provided such attack was otherwise lawful under international humanitarian law' is concerning from an international humanitarian law perspective.

36 See API, Art. 57(2)(b).
37 D. Fidler, above note 1, p. 532, note 29.
38 *Ibid*., p. 532, note 29; N. Lewer and N. Davidson, above note 5, p. 27, note 11.
39 European Working Group Non-Lethal Weapons Information Leaflet, April 2010, available at: http://waves.lima-city.de/pdf/leaflet.pdf.

Getting the balance right

There seems to be growing acceptance of the inevitability of the growth in and use of non-lethal weapons technology. Maj. Gen. Peter Chiarelli, US Army, notes:

> we are good at lethal effects; but in a counterinsurgency, non-lethal effects are as important . . . non-lethal effects are critical to winning the war in Iraq. So, if we are really serious about fighting an insurgency, we have to change our culture and accept the importance, and sometime preeminence, of non-lethal effects.[40]

The inevitability of their development and availability is not necessarily a bad thing, but must be balanced against the imperative to preserve the principles of international humanitarian law. The Geneva Conventions have been accepted by every nation in the world. Far from perfect, these documents contain some very basic provisions for the preservation of humanity in times of armed conflict. They should not be tampered with, for fear of weakening what protections currently exist. Starting again with the fundamental rules of international humanitarian law would set the cause back rather than forward.

Further, it is worth noting that while we may face a number of new challenges today, there is a 'remarkable consistency between age old moral principles and the modern rules of international law'.[41] That such principles, now rules, have stood the test of time suggests that there is merit in appreciating that they probably will continue to endure. As Mayer notes, the traditional approach may be the best:

> Requiring soldiers to use lethal weapons, when this may potentially cause greater harm to the non-combatants, seems to violate [non-combatant immunity]. However, when due care is taken to minimize non-combatant causalities . . . directly attacking the guerrillas with lethal weapons (that are capable of precision targeting) is the course of action most in line with [non-combatant immunity].[42]

Conclusion

Col. George Fenton, Director, Joint Non-Lethal Weapons Directorate, United States Department of Defense is quoted as saying he would like some magic dust to put everyone to sleep – combatant and non-combatant alike.[43] His approach might be the best way to minimize suffering in wartime, given humanity's propensity to go to war against each other. It is clear that we have failed to move on from Dunant's observations in 1862: 'in an age when we hear so much of progress and civilisation and since unhappily we cannot always avoid wars, the attempt must be made to

40 Massimo Annati, 'Non-lethal weapons revisited', in *Military Technology*, March 2007, p. 82.
41 D. Fidler, above note 29, p. 195.
42 C. Mayer, above note 19, p. 227.
43 Cited in D. Fidler, above note 29, p. 204.

prevent or to at least alleviate the horrors of war.'[44] In light of this, it is imperative to the preservation of the rules proposed by Dunant (which have served humanity over the past 150 years) that the prohibitions against any weapon, including those of a non-lethal nature, being targeted against non-combatants in armed conflict not be weakened. This is so even if it is thought that a moral 'greater good' justification can be formulated. The potential for abuse of this slippery slope is just too great.

The European Working Group Non-Lethal Weapons notes:

> Development of new non-lethal technologies will allow military and law enforcement personnel to exploit alternative means of countering potentially hazardous threats, expanding their capability with new options that offer an acceptable alternative to lethal force.[45]

This is true. Non-lethal weapons can be employed on the battlefield in the interests of humanity. The proviso being that the rules of international humanitarian law remain central to the use of force – lethal and non-lethal – in times of armed conflict.

44 Henry Dunant, *A Memory of Solferino*, ICRC, Geneva, 1862.
45 European Working Group, above note 39.

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making

Peter Asaro

Prof. Asaro is a philosopher of technology who has worked in artificial intelligence, neural networks, natural language processing, and robot vision research. He is an Affiliate Scholar at Stanford Law School's Center for Internet and Society, Co-Founder and Vice-Chair of the International Committee for Robot Arms Control, and the Director of Graduate Programs for the School of Media Studies at The New School for Public Engagement in New York City.

Abstract

This article considers the recent literature concerned with establishing an international prohibition on autonomous weapon systems. It seeks to address concerns expressed by some scholars that such a ban might be problematic for various reasons. It argues in favour of a theoretical foundation for such a ban based on human rights and humanitarian principles that are not only moral, but also legal ones. In particular, an implicit requirement for human judgement can be found in international humanitarian law governing armed conflict. Indeed, this requirement is implicit in the principles of distinction, proportionality, and military necessity that are found in international treaties, such as the 1949 Geneva Conventions, and firmly established in international customary law. Similar principles are also implicit in international human rights law, which ensures certain human rights for all people, regardless of national origins or local laws, at all times. I argue that the human rights to life and due process, and the limited conditions under which they can be

doi:10.1017/S1816383112000768

overridden, imply a specific duty with respect to a broad range of automated and autonomous technologies. In particular, there is a duty upon individuals and states in peacetime, as well as combatants, military organizations, and states in armed conflict situations, not to delegate to a machine or automated process the authority or capability to initiate the use of lethal force independently of human determinations of its moral and legal legitimacy in each and every case. I argue that it would be beneficial to establish this duty as an international norm, and express this with a treaty, before the emergence of a broad range of automated and autonomous weapons systems begin to appear that are likely to pose grave threats to the basic rights of individuals.

Keywords: robots, drones, autonomous weapon systems, automation, lethal decision-making, human rights, arms control.

In September 2009, the International Committee for Robot Arms Control (ICRAC)[1] was formed by Jürgen Altmann, Noel Sharkey, Rob Sparrow, and me. Shortly thereafter we issued a mission statement that included a call for discussion about the establishment of an international prohibition on autonomous weapon systems:

> Given the rapid pace of development of military robotics and the pressing dangers that these pose to peace and international security and to civilians in war, we call upon the international community to urgently commence a discussion about an arms control regime to reduce the threat posed by these systems. We propose that this discussion should consider the following: The prohibition of the development, deployment and use of armed autonomous unmanned systems; machines should not be allowed to make the decision to kill people.[2]

Since then, the issue has been taken up by philosophers, legal scholars, military officers, policymakers, scientists, and roboticists. The initial discussion has focused on the inability of existing autonomous weapon systems to meet the legal requirements of international humanitarian law (IHL), and conjectures as to the possibility that future technologies may, or may not, be able to meet these requirements. Of particular concern has been whether autonomous systems are capable of satisfying the principles of distinction and proportionality required by the Geneva Conventions, and whether it will be possible to hold anyone responsible for any wrongful harms the systems might cause. On the basis of the initial discussions, attention has begun to turn to the question of whether IHL needs to be

1 See www.icrac.net.

2 Jürgen Altmann, Peter Asaro, Noel Sharkey and Robert Sparrow, *Mission Statement of the International Committee for Robot Arms Control*, 2009, available at: http://icrac.net/statements/ (this and all links last visited June 2012).

supplemented with an international treaty that explicitly prohibits these technologies. While the vast majority of people and a number of scholars, lawyers, military officers, and engineers agree that lethal systems should not be autonomous, there are some who take the position that an international prohibition on autonomous weapon systems may be premature, unnecessary, or even immoral.[3] I believe that this latter position is mistaken, and propose that we must act soon to prohibit these systems. I will argue that we have moral and legal duties to prevent the delegation of lethal authority to unsupervised non-human systems, and to invest our science and engineering research and development resources in the enhancement of the ethical performance of human decision-makers. To support this argument, this article will supply a theoretical foundation for an international ban on autonomous weapon systems based on international human rights law (IHRL) and IHL. In addition to being enshrined in and protected by a large body of international and domestic law, human rights also have a moral status independent of existing law, and thus can provide sound guidance for the extension of the law to deal with the issues raised by emerging technologies. I will argue that an international ban on autonomous weapon systems can be firmly established on the principle that the authority to decide to initiate the use of lethal force cannot be legitimately delegated to an automated process, but must remain the responsibility of a human with the duty to make a considered and informed decision before taking human lives.

This principle has implications for a broad range of laws, including domestic laws, IHRL, and IHL. Insofar as the current interest in developing autonomous weapon systems is motivated primarily by military applications, I will focus on the IHL implications. However, the same principle would apply to the use of autonomous weapon systems by states for domestic policing, crowd control, border control, guarding prisoners, securing facilities and territory, or other potentially lethal activities, as well as to their use by individuals or organizations for a broad range of security applications involving the use of force. Similarly, I will focus on the human right to life, though similar arguments might be made regarding automated decisions to override or deny other human rights, in automating activities such as: arrest, detention, and restriction of movement; search, surveillance and tracking; deportation; eviction and foreclosure; denial of healthcare, public assembly, freedoms of press and speech, voting rights; and other civil, political, economic, social, and cultural rights.[4]

3 Ronald C. Arkin, *Governing Lethal Behavior in Autonomous Robots*, CRC Press, 2009; Gary Marchant, Braden Allenby, Ronald C. Arkin, Edward T. Barrett, Jason Borenstein, Lyn M. Gaudet, Orde F. Kittrie, Patrick Lin, George R. Lucas, Richard M. O'Meara and Jared Silberman, 'International governance of autonomous military robots', in *Columbia Science and Technology Law Review*, 30 December 2010, available at: http://ssrn.com/abstract=1778424; Kenneth Anderson and Matthew C. Waxman, 'Law and ethics for robot soldiers', in *Policy Review*, 28 April 2012, available at: http://ssrn.com/abstract=2046375.

4 The human rights currently recognized in international law include, but are not limited to, the rights enshrined in the United Nations International Bill of Human Rights, which contains the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights.

Autonomous weapon systems

Recent armed conflicts have seen an increased use of highly automated technologies, the most conspicuous being the use of armed, remotely piloted drones by the US military (among others) in a number of countries. These combat aircraft are capable of numerous sophisticated automated flight processes, including fully automated take-off and landing, GPS waypoint finding, and maintaining an orbit around a GPS location at a designated altitude, as well as numerous automated image collection and processing capabilities. While these systems are highly *automated*, they are not considered to be *autonomous* because they are still operated under human supervision and direct control.[5] Moreover, despite being armed with weapons that have some automated capabilities, such as laser-guided missiles and GPS-guided bombs, these systems still rely on direct human control over all targeting and firing decisions. The crucial concern of this article is with the legal and ethical ramifications of automating these targeting and firing decisions. We can thus define an 'autonomous weapon system' as any system that is capable of targeting and initiating the use of potentially lethal force without direct human supervision and direct human involvement in lethal decision-making.[6] Under this definition, current remote-piloted aircraft, such as Predator and Reaper drones, are not autonomous weapon systems. However, it is becoming increasingly clear that those activities that currently remain under human control might be automated in the near future, making possible the elimination of direct human involvement in target selection and decisions to engage targets with lethal force. Remote-piloted aircraft are not the only concern, as there are now numerous land, sea, and submarine systems that might also be armed, as well as fixed defensive systems, such as gun turrets and sentries, and various modes of cyber attack, which might be similarly automated so as to be capable of delivering lethal force without the direct involvement of human beings in selecting targets or authorizing the use of lethal force against a target.

While there are various examples of military weapons and practices that, arguably, do not include direct human involvement in lethal decision-making, this

5 The term 'autonomous' is used by engineers to designate systems that operate without direct human control or supervision. Engineers also use the term 'automated' to distinguish unsupervised systems or processes that involve repetitive, structured, routine operations without much feedback information (such as a dishwasher), from 'robotic' or 'autonomous' systems that operate in dynamic, unstructured, open environments based on feedback information from a variety of sensors (such as a self-driving car). Regardless of these distinctions, all such systems follow algorithmic instructions that are almost entirely fixed and deterministic, apart from their dependencies on unpredictable sensor data, and narrowly circumscribed probabilistic calculations that are sometimes used for learning and error correction.

6 I use the term 'autonomous weapon system' rather than simply 'autonomous weapon' to indicate that the system may be distributed amongst disparate elements that nonetheless work together to form an autonomous weapon system. For instance, a computer located almost anywhere in the world could receive information from a surveillance drone, and use that information to initiate and direct a strike from a guided weapon system at yet another location, all without human intervention or supervision, thereby constituting an autonomous weapon system. That is, the components of an autonomous weapon system – the sensors, autonomous targeting and decision-making, and the weapon – need not be directly attached to each other or co-located, but merely connected through communications links.

new wave of technological capability has raised serious concerns and trepidation amongst both the international law community and military professionals as to the moral and legal legitimacy of such systems. As Dr. Jakob Kellenberger, past president of the International Committee of the Red Cross (ICRC), expressed at a conference in San Remo, Italy, in September 2011:

> A truly autonomous system would have artificial intelligence that would have to be capable of implementing IHL. While there is considerable interest and funding for research in this area, such systems have not yet been weaponised. Their development represents a monumental programming challenge that may well prove impossible. The deployment of such systems would reflect a paradigm shift and a major qualitative change in the conduct of hostilities. It would also raise a range of fundamental legal, ethical and societal issues which need to be considered before such systems are developed or deployed. A robot could be programmed to behave more ethically and far more cautiously on the battlefield than a human being. But what if it is technically impossible to reliably program an autonomous weapon system so as to ensure that it functions in accordance with IHL under battlefield conditions? [. . .] [A]pplying pre-existing legal rules to a new technology raises the question of whether the rules are sufficiently clear in light of the technology's specific – and perhaps unprecedented – characteristics, as well as with regard to the foreseeable humanitarian impact it may have. In certain circumstances, states will choose or have chosen to adopt more specific regulations.[7]

As Kellenberger makes clear, there are serious concerns as to whether autonomous technologies will be technically capable of conforming to existing IHL. While many military professionals recognize the technological movement towards greater autonomy in lethal weapons systems, most express strong ethical concerns, including policymakers at the US Office of the Secretary of Defense:

> Restraints on autonomous weapons to ensure ethical engagements are essential, but building autonomous weapons that *fail safely* is the harder task. The wartime environment in which military systems operate is messy and complicated, and autonomous systems must be capable of operating appropriately in it. Enemy adaptation, degraded communications, environmental hazards, civilians in the battlespace, cyber attacks, malfunctions, and 'friction' in war all introduce the possibility that autonomous systems will face unanticipated situations and may act in an unintended fashion. Because they lack a broad contextual intelligence, or common sense, on par with humans, even relatively sophisticated algorithms are subject to failure if they face situations outside their intended design parameters. The complexity of modern computers complicates this problem by making it difficult to anticipate all

7 Jakob Kellenberger, 'Keynote Address', International Humanitarian Law and New Weapon Technologies, 34th Round Table on Current Issues of International Humanitarian Law, San Remo, Italy, 8–10 September 2011, pp. 5–6, available at: http://www.iihl.org/iihl/Documents/JKBSan%20Remo%20Speech.pdf.

possible glitches or emergent behavior that may occur in a system when it is put into operation.[8]

Because even 'artificially intelligent' autonomous systems must be pre-programmed, and will have only highly limited capabilities for learning and adaptation at best, it will be difficult or impossible to design systems capable of dealing with the fog and friction of war. When we consider the implications of this for protecting civilians in armed conflict, this raises several ethical and legal questions, particularly in relation to conforming to the IHL requirements of the principles of distinction, proportionality, and military necessity, and the difficulty of establishing responsibility and accountability for the use of lethal force.

Autonomous weapon systems raise a host of ethical and social concerns, including issues of asymmetric warfare and risk redistribution from combatants to civilians and the potential to lower the thresholds for nations to start wars.[9] Insofar as such weapons tend to remove the combatants who operate them from area of conflict and reduce the risks of causalities for those who possess them, they tend to also reduce the political costs and risks of going to war. This could result in an overall lowering of the threshold of going to war. Autonomous weapon systems also have the potential to cause regional or global instability and insecurity, to fuel arms races, to proliferate to non-state actors, or initiate the escalation of conflicts outside of human political intentions. Systems capable of initiating lethal force without human supervision could do so even when political and military leadership has not deemed such action appropriate, resulting in the unintended initiation or escalation of conflicts outside of direct human control.[10] Thus, these systems pose a serious threat to international stability and the ability of international bodies to manage conflicts.

In terms of the legal acceptability of these systems under existing IHL,[11] the primary question appears to be whether autonomous systems will be able to satisfy the principles of distinction and proportionality.[12] Given the complexity of these

8 Paul Scharre, 'Why unmanned', in *Joint Force Quarterly*, Issue 61, 2nd Quarter, 2011, p. 92.

9 Peter Asaro, 'How just could a robot war be?', in Adam Briggle, Katinka Waelbers and Philip A. E. Brey (eds), *Current Issues in Computing And Philosophy*, IOS Press, Amsterdam, 2008, pp. 50–64, available at: http://peterasaro.org/writing/Asaro%20Just%20Robot%20War.pdf.

10 By analogy, one should consider the stock market 'Flash Crash' of 6 May 2010, in which automated high-frequency trading systems escalated and accelerated a 1,000-point drop in the Dow Jones average (9%), the single largest drop in history. See *Wikipedia*, 'Flash Crash', available at: http://en.wikipedia.org/wiki/Flash_crash.

11 Noel Sharkey, 'Death strikes from the sky: the calculus of proportionality', in *IEEE Technology and Society Magazine*, Vol. 28, No. 1, 2009, pp. 16–19; Noel Sharkey, 'Saying "no!" to lethal autonomous targeting', in *Journal of Military Ethics*, Vol. 9, No. 4, 2010, pp. 369–383; Markus Wagner, 'Taking humans out of the loop: implications for international humanitarian law', in *Journal of Law Information and Science*, Vol. 21, 2011, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1874039; Matthew Bolton, Thomas Nash and Richard Moyes, 'Ban autonomous armed robots', Article36.org, 5 March 2012, available at: http://www.article36.org/statements/ban-autonomous-armed-robots.

12 See in particular, Articles 51 and 57 of Additional Protocol I to the Geneva Conventions address the protection of the civilian population and precautions in attack. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, 8 June 1977, 1125 UNTS 3 (entered into force 7 December 1978), available at: http://www2.ohchr.org/english/law/protocol1_2.htm.

systems, and our inability to foresee how they might act in complex operational environments, unanticipated circumstances, and ambiguous situations, there is a further difficulty – how we can test and verify that a newly designed autonomous weapon system meets the requirements imposed by IHL, as required by Article 36 of Additional Protocol I,[13] and more generally how to govern the increasingly rapid technological innovation of new weapons and tactics.[14]

There is a separate concern that such systems may not have an identifiable operator in the sense that no human individual could be held responsible for the actions of the autonomous weapon system in a given situation, or that the behaviour of the system could be so unpredictable that it would be unfair to hold the operator responsible for what the system does.[15] Such systems might thus eliminate the possibility of establishing any individual criminal responsibility that requires moral agency and a determination of *mens rea*.[16] In the event of an atrocity or tragedy caused by an autonomous weapon system under the supervision or command of a human operator they may also undermine command responsibility and the duty to supervise subordinates, thus shielding their human commanders from what might have otherwise been considered a war crime. It is thus increasingly important to hold states accountable for the design and use of such systems, and to regulate them at an international level.

We are at a juncture at which we must decide how we, as an international community, will treat these systems. Will we treat them as new extensions of old technologies, or as a qualitative shift to a new kind of technology? Is current IHL and IHRL sufficient to deal with autonomous lethal technologies, or are they in need of minor extensions, or major revisions? Is a ban on autonomous weapon systems desirable, or might it disrupt the development of weapons with greater capabilities for respecting moral and legal norms?

It is my view that autonomous weapon systems represent a qualitative shift in military technology, precisely because they eliminate human judgement in the initiation of lethal force. Therefore they threaten to undermine human rights in the absence of human judgement and review. There are good reasons to clarify IHL and IHRL by explicitly codifying a prohibition on the use of autonomous weapon systems. Moreover, these reasons stand up against all of the criticisms offered thus far. The benefits to such a clarification and codification include:

1) avoiding various slippery slopes towards autonomous weapon systems by drawing a principled bound on what can and cannot be automated;

13 The full text of Article 36 of Additional Protocol I on New Weapons reads: 'In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party'.

14 Richard M. O'Meara, 'Contemporary governance architecture regarding robotics technologies: an assessment', in Patrick Lin, Keith Abney and George Bekey, *Robot Ethics*, MIT Press, Cambridge MA, 2011, pp. 159–168.

15 Robert Sparrow, 'Killer robots', in *Journal of Applied Philosophy*, Vol. 24, No. 1, 2007, pp. 62–77.

16 M. Wagner, above note 11, p. 5.

2) shaping future investments in technology development towards more human-centred designs capable of enhancing ethical and legal conduct in armed conflicts;
3) stemming the potential for more radical destabilizations of the ethical and legal norms governing armed conflict that these new technologies might pose; and
4) establishing the legal principle that automated processes do not satisfy the moral requirements of due consideration when a human life is at stake.

It would therefore be desirable for the international community to move to establish an international ban on autonomous weapon systems on the basis of protecting human rights norms as well as other norms protecting the individual.

Lethal decision-making

In an argument that the use of autonomous weapon systems is morally and legally impermissible, it is necessary to elucidate how autonomous weapon systems fail to meet the necessary and sufficient conditions for permissible killing in armed conflict. It is also necessary to refine the notion of an autonomous weapon system. For now it is sufficient to define the class of autonomous weapon systems as any automated system that can initiate lethal force without the specific, conscious, and deliberate decision of a human operator, controller, or supervisor.

Admittedly, such systems are not unprecedented in the sense that there are various sorts of precursors that have been used in armed conflicts, including mines and other victim-activated traps, as well as certain guided missiles and some automatic defence systems. Indeed, there is a sense in which these systems are not themselves 'weapons' so much as they are automated systems armed with, or in control of, weapons. They thus present a challenge to traditional modes of thought regarding weapons and arms control, which tend to focus on the weapon as a tool or instrument, or upon its destructive effects. Rather, autonomous weapon systems force us to think in terms of 'systems' that might encompass a great variety of configurations of sensors, information processing, and weapons deployment, and to focus on the process by which the use of force is initiated.[17]

Within the US military there has been a policy to follow a human-in-the-loop model when it comes to the initiation of lethal force. The phrase 'human-in-the-loop' comes from the field of human factors engineering, and indicates that a human is an integral part of the system. When it comes to lethal force, the crucial system is the one that contains the decision-making cycle in which any determination to use lethal force is made. In military jargon, this decision cycle is referred to as the 'kill chain', defined in the US Air Force as containing six steps:

17 In the language of Article 36 of Additional Protocol I to the Geneva Conventions, autonomous weapon systems are subject to review on the basis of being a 'new weapon, means or method of warfare'. This implies that using an existing approved weapon in a new way, i.e. with autonomous targeting or firing, is itself subject to review as a new means or method.

find, fix, track, target, engage and assess.[18] There has been recent discussion of moving to a 'human-on-the-loop' model, in which a human might supervise one or more systems that automate many of the tasks in this six-step cycle. This shift appears to create a middle position between the direct human control of the human-in-the-loop model and an autonomous weapons system. However, the crucial step that determines whether a given system is an autonomous weapon system or not is whether it automates either the target or the engage steps independently of direct human control. We can thus designate the class of systems capable of selecting targets and initiating the use of potentially lethal force without the deliberate and specific consideration of humans as being 'autonomous weapon systems'.

This definition recognizes that the fundamental ethical and legal issue is establishing the causal coupling of automated decision-making to the use of a weapon or lethal force, or conversely the decoupling of human decision-making from directly controlling the initiation of lethal force by an automated system. It is the delegation of the human decision-making responsibilities to an autonomous system designed to take human lives that is the central moral and legal issue.

Note that including a human in the lethal decision process is a necessary, but not a sufficient requirement. A legitimate lethal decision process must also meet requirements that the human decision-maker involved in verifying legitimate targets and initiating lethal force against them be allowed sufficient time to be deliberative, be suitably trained and well informed, and be held accountable and responsible. It might be easy to place a poorly trained person in front of a screen that streams a list of designated targets and requires them to verify the targets, and press a button to authorize engaging those targets with lethal force. Such a person may be no better than an automaton when forced to make decisions rapidly without time to deliberate, or without access to relevant and sufficient information upon which to make a meaningful decision, or when subjected to extreme physical and emotional stress. When evaluating the appropriateness of an individual's decision, we generally take such factors into account, and we are less likely to hold them responsible for decisions made under such circumstances and for any unintended consequences that result, though we do still hold them accountable. Because these factors diminish the responsibility of decision-makers, the design and use of systems that increase the likelihood that decision-making will have to be done under such circumstances is itself irresponsible. I would submit that, when viewed from the perspective of engineering and design ethics, intentionally designing systems that lack responsible and accountable agents is in and of itself unethical, irresponsible, and immoral. When it comes to establishing the standards against which we evaluate lethal decision-making, we should not confuse the considerations we grant to humans acting under duress with our ideals for such standards. Moreover, the fact that we can degrade human performance in such decisions to the level of autonomous systems does not mean we should lower our standards of judging those decisions.

18 Julian C. Cheater, 'Accelerating the kill chain via future unmanned aircraft', Blue Horizons Paper, Center for Strategy and Technology, Air War College, April 2007, p. 5, available at: http://www.au.af.mil/au/awc/awcgate/cst/bh_cheater.pdf.

While the detailed language defining autonomous weapon systems in an international treaty will necessarily be determined through a process of negotiations, the centrepiece of such a treaty should be the establishment of the principle that human lives cannot be taken without an informed and considered human decision regarding those lives in each and every use of force, and any automated system that fails to meet that principle by removing humans from lethal decision processes is therefore prohibited. This proposal is novel in the field of arms control insofar as it does not focus on a particular weapon, but rather on the manner in which the decision to use that weapon is made. Previous arms control treaties have focused on specific weapons and their effects, or the necessarily indiscriminate nature of a weapon. A ban on autonomous weapons systems must instead focus on the delegation of the authority to initiate lethal force to an automated process not under direct human supervision and discretionary control.

The requirement for human judgement in legal killing

In order for the taking of a human life in armed conflict to be considered legal it must conform to the requirements of IHL. In particular, parties to an armed conflict have a duty to apply the principles of distinction and proportionality. There has been much discussion regarding the ability of autonomous systems to conform to these principles. The most ambitious proposal has been that we may be able to program autonomous weapon systems in such a way that they will conform to the body of IHL, as well as to the specific rules of engagement (ROE) and commander's orders for a given mission.[19] Based in the tradition of constraint-based programming, the proposal is that IHL can be translated into programming rules that strictly determine which actions are prohibited in a given situation. Thus a hypothetical 'ethical governor' could engage to prevent an autonomous weapon system from conducting an action that it determines to be explicitly prohibited under IHL. Arkin further argues that because autonomous weapon systems could choose to sacrifice themselves in situations where we would not expect humans to do the same, these systems might avoid many of the mistakes and failings of humans, and they might accordingly be better at conforming to the rules of IHL than humans.

On its surface, this proposal is quite appealing, and even Kellenberger recognizes its seductive appeal:

> When we discuss these new technologies, let us also look at their possible advantages in contributing to greater protection. Respect for the principles of distinction and proportionality means that certain precautions in attack, provided for in Article 57 of Additional Protocol I, must be taken. This includes the obligation of an attacker to take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to

19 R. C. Arkin, above note 3, pp. 71–91.

> minimizing, incidental civilian casualties and damages. In certain cases cyber operations or the deployment of remote-controlled weapons or robots might cause fewer incidental civilian casualties and less incidental civilian damage compared to the use of conventional weapons. Greater precautions might also be feasible in practice, simply because these weapons are deployed from a safe distance, often with time to choose one's target carefully and to choose the moment of attack in order to minimise civilian casualties and damage. It may be argued that in such circumstances this rule would require that a commander consider whether he or she can achieve the same military advantage by using such means and methods of warfare, if practicable.[20]

While it would indeed be advantageous to enhance the protection of civilians and civilian property in future armed conflicts, we must be careful about the inferences we draw from this with regard to permitting the use of autonomous weapon systems. There are a great many assumptions built into this seemingly simple argument, which might mislead us as to the purpose and meaning of IHL.

During armed conflict, the ultimate goal of IHL is to protect those who are not, or are no longer, taking direct part in the hostilities, as well as to restrict the recourse to certain means and methods of warfare. It is tempting to think that this can be objectively and straightforwardly measured. We might like to believe that the principle of distinction is like a sorting rule – that the world consists of civilians and combatants and there is a rule, however complex, that can definitively sort each individual into one category or the other.[21] But it is much more complicated than this. Let's take as an example the difficulty of determining what 'a civilian participating in hostilities' means. The ICRC has laid out a carefully considered set of guidelines for what constitutes 'an act of direct participation in hostilities', and under which a civilian is not afforded the protections normally granted to civilians under IHL.[22] These guidelines set forth three requirements that must be satisfied in order to conclude that a civilian is a legitimate target: 1) threshold of harm, 2) direct causation, and 3) belligerent nexus. Each is elaborated in the ICRC Guidelines, but for present purposes a short summary shall suffice:

> For a specific act to reach the *threshold of harm* required to qualify as direct participation in hostilities, it must be likely to adversely affect the military operations or military capacity of a party to an armed conflict. In the absence of military harm, the threshold can also be reached where an act is likely to inflict death, injury, or destruction on persons or objects protected against direct attack. In both cases, acts reaching the required threshold of harm can only

20 J. Kellenberger, above note 7, p. 6

21 Indeed, there is a tendency in the literature on autonomous weapons to refer to 'discrimination' rather than the principle of distinction, which connotes the 'discrimination task' in cognitive psychology and artificial intelligence. See Noel Sharkey's opinion note in this volume.

22 Nils Mezler, *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*, ICRC, Geneva, 2009, p. 20, available at: http://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf.

> amount to direct participation in hostilities if they additionally satisfy the requirements of direct causation and belligerent nexus. . . .
>
> The requirement of *direct causation* is satisfied if either the specific act in question, or a concrete and coordinated military operation of which that act constitutes an integral part, may reasonably be expected to directly – in one causal step – cause harm that reaches the required threshold. However, even acts meeting the requirements of direct causation and reaching the required threshold of harm can only amount to direct participation in hostilities if they additionally satisfy the third requirement, that of belligerent nexus. . . .
>
> In order to meet the requirement of *belligerent nexus*, an act must be specifically designed to directly cause the required threshold of harm in support of a party to an armed conflict and to the detriment of another. As a general rule, harm caused (A) in individual self-defence or defence of others against violence prohibited under IHL, (B) in exercising power or authority over persons or territory, (C) as part of civil unrest against such authority, or (D) during inter-civilian violence lacks the belligerent nexus required for a qualification as direct participation in hostilities. . . .
>
> Applied in conjunction, the three requirements of *threshold of harm, direct causation* and *belligerent nexus* permit a reliable distinction between activities amounting to direct participation in hostilities and activities which, although occurring in the context of an armed conflict, are not part of the conduct of hostilities and, therefore, do not entail loss of protection against direct attack. Even where a specific act amounts to direct participation in hostilities, however, the kind and degree of force used in response must comply with the rules and principles of IHL and other applicable international law.[23]

These guidelines represent an attempt to articulate a means by which to determine who is a legitimate target and who is not. And yet these are not even called rules – they are called guidelines because they help guide a moral agent through multiple layers of interpretation and judgement. To determine whether a specific individual in a specific circumstance meets each of these requirements requires a sophisticated understanding of a complex situation including: the tactical and strategic implications of a potential harm, as well as the status of other potentially threatened individuals; the nature of causal structures and relations and direct causal implications of someone's actions; the sociocultural and psychological situation in which that individual's intentions and actions qualify as military actions and not, for instance, as the exercise of official duties of authority or personal self-defence.

What does it really mean to say that we can program the rules of IHL into a computer? Is it simply a matter of turning laws written to govern human actions into programmed codes to constrain the actions of machine? Should the next additional protocol to the Geneva Conventions be written directly into computer code? Or is there something more to IHL that cannot be programmed? It is tempting to take an engineering approach to the issue and view the decisions and

23 *Idem*., pp. 50–64.

actions of a combatant as a 'black box', and compare the human soldier to the robotic soldier and claim that the one that makes fewer mistakes according to IHL is the 'more ethical' soldier. This has been a common argument strategy in the history of artificial intelligence as well.

There are really two questions here, however. The empirical question is whether a computer, machine, or automated process could make each of these decisions of life and death and achieve some performance that is deemed acceptable. But the moral question is whether a computer, machine or automated process ought to make these decisions of life and death at all. Unless we can prove in principle that a machine should not make such decisions, we are left to wonder if or when some clever programmers might be able to devise a computer system that can do these things, or at least when we will allow machines to make such decisions.

The history of artificial intelligence is instructive here, insofar as it tells us that such problems are, in general, computationally intractable, but if we can very carefully restrict and simplify the problem, we might have better success. We might also, however, compare the sort of problems artificial intelligence has been successful at, such as chess, with the sort of problems encountered in applying IHL requirements. While IHL requirements are in some sense 'rules', they are quite unlike the rules of chess in that they require a great deal of interpretative judgement in order to be applied appropriately in any given situation. Moreover, the context in which the rules are being applied, and the nature and quality of the available information, and alternative competing or conflicting interpretations, might vary widely from day to day, even in the same conflict, or even in the same day.

We might wish to argue that intelligence is uniquely human, but if one can define it specifically enough, or reduce it to a concrete task, then it may be possible to program a computer to do that task better. When we do that, we are necessarily changing the definition of intelligence by redefining a complex skill into the performance of a specific task. Perhaps it is not so important whether we redefine intelligence in light of developments in computing, though it certainly has social and cultural consequences. But when it comes to morality, and the taking of human lives, do we really want to redefine what it means to be moral in order to accommodate autonomous weapon systems? What is at stake if we allow automated systems the authority to decide whether to kill someone? In the absence of human judgement, how can we ensure that such killing is not arbitrary?

Automating the rules of IHL would likely undermine the role they play in regulating ethical human conduct. It would also explain why designers have sought to keep humans-in-the-loop for the purposes of disambiguation and moral evaluation. As Sir Brian Burridge, commander of the British Royal Air Force in Iraq from 2003 to 2005, puts it:

> Under the law of armed conflict, there remains the requirement to assess proportionality and within this, there is an expectation that the human at the end of the delivery chain makes the last assessment by evaluating the situation using rational judgement. Post-modern conflicts confront us … with ambiguous non-linear battlespaces. And thus, we cannot take the human, the

> commander, the analyst, those who wrestle with ambiguity, out of the loop. The debate about the human-in-the-loop goes wider than that.[24]

The very nature of IHL, which was designed to govern the conduct of humans and human organizations in armed conflict, presupposes that combatants will be human agents. It is in this sense anthropocentric. Despite the best efforts of its authors to be clear and precise, applying IHL requires multiple levels of interpretation in order to be effective in a given situation. IHL supplements its rules with heuristic guidelines for human agents to follow, explicitly requires combatants to reflexively consider the implications of their actions, and to apply compassion and judgement in an explicit appeal to their humanity. In doing this, the law does not impose a specific calculation, but rather, it imposes a duty on combatants to make a deliberate consideration as to the potential cost in human lives and property of their available courses of action.

Justice cannot be automated

Law is by its essential nature incomplete and subject to interpretation and future review. However careful, thoughtful, and well intentioned a law or rule might be, the legal system is not, and cannot be, perfect. It is a dynamically evolving system, and is designed as such with human institutions to manage its application in the world of human affairs. There are a number of human agents – judges, prosecutors, defenders, witnesses, juries – all of whom engage in complex processes of interpretation and judgement to keep the legal system on track. In short, they are actively engaged in assessing the match between an abstract set of rules and any given concrete situation. The right to due process is essentially the right to have such a deliberative process made publicly accountable.

We could imagine a computer program to replace these human agents, and to automate their decisions. But this, I contend, would fundamentally undermine the right to due process. That right is essentially the right to question the rules and the appropriateness of their application in a given circumstance, and to make an appeal to informed human rationality and understanding. Do humans in these positions sometimes make mistakes? Yes, of course they do. Human understanding, rationality, and judgement exceed any conceivable system of fixed rules or any computational system, however. Moreover, when considering the arguments in a given case, the potential for appeals to overturn judicial decisions, and the ways in which opinions and case law inform the interpretation of laws, we must recognize that making legal judgements requires considering different, incompatible, and even contradictory perspectives, and drawing insight from them. There are no known computational or algorithmic systems that can do this, and it might well be impossible for them to do so.

24 Brian Burridge, 'UAVs and the dawn of post-modern warfare: a perspective on recent operations', in *RUSI Journal*, Vol. 148, No. 5, October 2003, pp. 18–23.

More importantly, human judgement is constitutive of the system of justice. That is, if any system of justice is to apply to humans, then it must rely upon human reason. Justice itself cannot be delegated to automated processes. While the automation of various tasks involved in administrative and legal proceedings may enhance the ability or efficiency of humans to make their judgements, it cannot abrogate their duty to consider the evidence, deliberate alternative interpretations, and reach an informed opinion. Most efforts at automating administrative justice have not improved upon human performance, in fact, but have greatly degraded it.[25] To automate these essential aspects of human judgement in the judicial process would be to dehumanize justice, and ought to be rejected in principle.

In saying that the automation of human reasoning in the processes of justice ought to be rejected in principle, I mean that there is no automated system, and no measure of performance that such a system could reach, that we should accept as a replacement for a human. In short, when it comes to a system of justice, or the state, or their agents, making determinations regarding the human rights of an individual, the ultimate agents and officials of the state must themselves be human. One could argue for this principle on moral grounds, as well as on the legal grounds that it is constitutive of, and essential to, the system of justice itself independently of its moral standing.

Within the military there are many layers of delegated authority, from the commander-in-chief down to the private, but at each layer there is a responsible human to bear both the authority and responsibility for the use of force. The nature of command responsibility does not allow one to abdicate one's moral and legal obligations to determine that the use of force is appropriate in a given situation. One might transfer this obligation to another responsible human agent, but one then has a duty to oversee the conduct of that subordinate agent. Insofar as autonomous weapon systems are not responsible human agents, one cannot delegate this authority to them.

In this sense, the principle of distinction can be seen not simply as following a rule that sorts out combatants from civilians, but also of giving consideration to human lives that might be lost if lethal force is used. And in this regard, it is necessary for a human being to make an informed decision before that life can be taken. This is more obvious in proportionality decisions in which one must weigh the value of human lives, civilian and combatant, against the values of military objectives. None of these are fixed values, and in some ways these values are set by the very moral determinations that go into making proportionality judgements.

This is why we cannot claim that an autonomous weapon system would be morally superior to a human soldier on the basis that it might be technologically capable of making fewer errors in a discrimination task, or finding means of neutralizing military targets that optimally minimize the risk of disproportionate harms. This is not to say that these goals are not desirable. If technologies did exist

25 Danielle Keats Citron, 'Technological due process', in *Washington University Law Review*, Vol. 85, 2008, pp. 1249–1292.

that could distinguish civilians from combatants better than any human, or better than the average combatant, then those technologies should be deployed in a manner to assist the combatant in applying the principle of distinction, rather than used to eliminate human judgement. Similarly, if a technology were capable of determining a course of action which could achieve a military objective with minimal collateral damage, and minimize any disproportionate harms, then that technology could be employed by a human combatant charged with the duty of making an informed choice to initiate the use of lethal force in that situation.

Any automated process, however good it might be, and even if measurably better than human performance, ought to be subject to human review before it can legitimately initiate the use of lethal force. This is clearly technologically required for the foreseeable future because autonomous systems will not reach human levels of performance for some time to come. But more importantly, this is a moral requirement and, in many important instances, a legal requirement. I therefore assert that in general there is a duty not to permit autonomous systems to initiate lethal force without direct human supervision and control.

There are two basic strategies for arguing that autonomous weapons systems might provide a morally or legally superior means of waging war compared to current means of armed conflict. There are many variations of the argument, which I divide into two classes: 1) pragmatic arguments pointing to failures of lethal decision-making in armed conflict and arguing to possible/hypothetical technological improvements through automating these decisions,[26] and 2) arguing that insofar as such systems imply a reduced risk to combatants and/or civilians in general, as measured by fewer casualties, there is a moral imperative to use them. Such arguments have been made for precision weapons in the past,[27] and more recently for Predator drones and remote-operated lethality.[28]

Are more precise weapons more 'moral' than less precise weapons? It is easy enough to argue that given the choice between attacking a military target with a precision-guided munition with low risk of collateral damage, and attacking the same target by carpet bombing with a high risk or certainty of great collateral damage, one ought to choose the precision-guided munition. That is the moral and legal choice to make, all other things being equal. Of course, there is quite a bit that might be packed into the phrase 'all other things being equal'. Thus it is true that one should prefer a more precise weapon to a less precise weapon when deciding how to engage a target, but the weapon is not ethically independent of that choice. And ultimately it is the human agent who chooses to use the weapon that is judged to be moral or not. Even the most precise weapon can be used illegally and immorally. All that precision affords is a possibility for more ethical behaviour – it does not determine or guarantee it.

26 Ronald C. Arkin, 'Governing lethal behavior: embedding ethics in a hybrid deliberative/reactive robot architecture', Georgia Institute of Technology, Technical Report GUT-GVU-07-11, 2007, p. 11.

27 Human Rights Watch, 'International humanitarian law issues in the possible U.S. invasion of Iraq', in *Lancet*, 20 February 2003.

28 Bradley Jay Strawser, 'Moral predators: the duty to employ uninhabited aerial vehicles', in *Journal of Military Ethics*, Vol. 9, No. 4, 2010, pp. 342–368.

This may seem like a semantic argument, but it is a crucial distinction. We do not abrogate our moral responsibilities by using more precise technologies. But as with other automated systems, such as cruise control or autopilot, we still hold the operator responsible for the system they are operating, the ultimate decision to engage the automated system or to disengage it, and the appropriateness of these choices. Indeed, in most cases these technologies, as we have seen in the use of precision-guided munitions and armed drones, actually increase our moral burden to ensure that targets are properly selected and civilians are spared. And indeed, as our technologies increase in sophistication, we should design them so as to enhance our moral conduct.

There is something profoundly odd about claiming to improve the morality of warfare by automating humans out of it altogether, or at least by automating the decisions to use lethal force. The rhetorical strategy of these arguments is to point out the moral shortcomings of humans in war – acts of desperation and fear, mistakes made under stress, duress, and in the fog of war. The next move is to appeal to a technological solution that might eliminate such mistakes. This might sound appealing, despite the fact that the technology does not exist. It also misses two crucial points about the new kinds of automated technologies that we are seeing. First, that by removing soldiers from the immediate risks of war, which tele-operated systems do without automating lethal decisions, we can also avoid many of these psychological pressures and the mistakes they cause. Second, if there were an automated system that could outperform humans in discrimination tasks, or proportionality calculations, it could just as easily be used as an advisory system to assist and inform human decision-makers, and need not be given the authority to initiate lethal force independently of informed human decisions.[29]

Arguments against banning autonomous weapon systems

In a recent policy brief, Anderson and Waxman offer a criticism of proposals to ban autonomous weapon systems.[30] They conclude that while it is important to establish international norms regarding the use of autonomous weapon systems, a ban is not the best way to do it. There are, however, numerous problems with their argument and many of their conclusions. The main thrust of their argument is based in two assumptions:

> Recognizing the inevitable but incremental evolution of these technologies is key to addressing the legal and ethical dilemmas associated with them; US policy toward resolving those dilemmas should be built upon these assumptions. The certain yet gradual development and deployment of these systems, as well as the humanitarian advantages created by the precision of some systems,

29 Peter Asaro, 'Modeling the moral user: designing ethical interfaces for tele-operation', in *IEEE Technology & Society*, Vol. 28, No. 1, 2009, pp. 20–24, available at: http://peterasaro.org/writing/Asaro%20Modeling%20Moral%20User.pdf.

30 K. Anderson and M. C. Waxman, above note 3, p. 13.

> make some proposed responses – such as prohibitory treaties – unworkable as well as ethically questionable.[31]

Here we see several arguments being made against the proposal for an international prohibitory treaty. First, they insist upon starting from the assumptions that these technologies are inevitable, and that their development is incremental. Yet they provide no evidence or arguments to support either assumption, even though there are strong reasons to reject them. They then make a further argument that some of these systems may have humanitarian advantages, and thus prohibitions are both 'unworkable' and 'ethically questionable'. Having just explained why it is not 'ethically questionable' to argue that even the most precise autonomous weapon systems jeopardize human rights, I want to focus on their two preliminary assumptions and what they might mean for the practicality of an international prohibition.

Are autonomous weapon systems inevitable?

Why should we assume that autonomous weapon systems are inevitable? What might this actually mean? As a philosopher and historian of science and technology, I often encounter claims about the 'inevitability' of scientific discoveries or technological innovations. The popularity of such claims is largely due to the retrospective character of history, and applying our understanding of past technologies to thinking about the future. That is, it seems easy for us, looking back, to say that the invention of the light bulb, or the telephone, or whatever technology you prefer was inevitable – because it did in fact happen. It is hard to imagine what the world would be like if it had not happened. Yet when one looks carefully at the historical details, whether a technology succeeded technologically was in most cases highly contingent on a variety of factors. In most cases, the adoption of the technology was not guaranteed by the success of the innovation, and the means and manner of its eventual use always depended upon a great variety of social and cultural forces. Indeed, when we look at the great many technological failures, and indeed the many failed attempts to commercialize the light bulb before it finally succeeded, what becomes clear is that very few, if any, technologies can fairly be claimed to be 'inevitable'. And even the successful light bulb was dependent upon the innovation and development of electrical utilities, and a host of other electric appliances, such as toasters, for its widespread adoption. Technologies evolve much faster now, but they are just as dynamic and unpredictable.

Perhaps what Anderson and Waxman mean is that it seems very likely that these technologies will be developed. This seems more plausible. Indeed, simplistic systems can already implement the essential elements of an autonomous weapon system, though these would fail to meet the existing international legal standards of discrimination and proportionality.[32] But even ignoring the existing legal

31 *Idem*., p. 2.
32 M. Wagner, above note 11, pp. 5–9.

limitations, the fact that we can build autonomous lethal technologies does not mean we will use them. Given that various sorts of autonomous weapon systems are already possible, it might be claimed that it is their adoption that is inevitable. But to assume this would be glossing over the important differences between the invention of a technology and its widespread adoption in society. There are certainly some strong motivations for adopting such technologies, including the desire to reduce the risks to military personnel, as well as reduce the costs and number of people needed for various military operations and capabilities.

Or more strongly, Anderson and Waxman might mean that we should assume that it is inevitable that there will be autonomous weapon systems that are capable of meeting the requirements of some measure of discrimination and proportionality. But this is an empirical claim, about the capabilities of technologies that do not yet exist, being measured against a metric that does not yet exist. As a purely empirical question, these technologies may or may not come into existence and we may not even be able to agree upon acceptable metrics for evaluating their performance, so why should we believe that they are inevitable?[33]

The crucial question here is whether these technologies can meet the requirements of international law, and this is far from certain. The arguments claiming the ethical superiority of robotic soldiers sound suspiciously like claims from the early days of artificial intelligence that computers would someday beat human grandmasters at chess. And, forty years later than initial predictions, IBM's Deep Blue did manage to beat Gary Kasparov. But there are important differences between chess and IHL that are worth noting. Chess is a fairly well-defined rule-based game that is susceptible to computational analysis. Ultimately, the game of chess is not a matter of interpretation, nor is it a matter of social norms. International law, while it has rules, is not like chess. Law always requires interpretation and judgement in order to apply it to real world situations. These interpretations and judgements are aided by historical precedents and established standards, but they are not strictly determined by them. The body of case law, procedures, arguments, and appeals is able to defend old principles or establish new precedents, and thereby establish norms and principles, even as those norms and principles continue to grow in meaning over time.

Thus, insisting that autonomous weapon systems are inevitable is actually quite pernicious. On the one hand, this assumption would make the establishment of a ban seem automatically impractical or unworkable. That is, if we start from the assumption that the banned systems will exist and will be used, then why should we bother to ban them? But of course, they do not exist and are not being used, and even if they were being used already they could still be banned going forward. And far from being unworkable or impractical, a ban could be quite effective in shifting innovation trajectories towards more useful and genuinely ethical systems. It seems

33 For comparison, consider electric cars, a technology that has existed for a century. Even with the recent popularity of hybrid gas/electric cars, and some highly capable electric cars, few people would endorse the claim that our transition to electric cars is inevitable. And this is a technology that is already possible, i.e. it exists.

straightforward that we can define the class of autonomous weapon systems clearly enough, and then debate how a treaty might apply to, or exempt, certain borderline cases such as reactive armour, anti-ballistic missile defences, or supervisory systems. A ban cannot be expected to prohibit each and every use of automation in armed conflict, but rather to establish an international norm that says that it is illegitimate to use systems that make automated lethal decisions. The international bans on landmines and cluster munitions may have not completely eliminated landmines and cluster munitions and their use in armed conflict, but they have made it more difficult for manufacturers to produce them profitably, and for militaries to use them without repercussions in the international community.

Moreover, starting from an assumption of the inevitability of autonomous weapon systems appears to make the acceptability of such systems a foregone conclusion. Yet what is ultimately at issue here is what the international standards of acceptability will be – what the international community will consider the norms of conduct to be. To assume the inevitability of the development and use of the technologies in question is to close off further discussion on the wisdom and desirability of pursuing, developing, and using these technologies. In short, the development and use of autonomous weapon systems is not inevitable – no technology is. Yes, they are possible; if they were not then there would be no need to ban them, but their developments still requires great investment. And even if we may not be able to prevent the creation of certain technologies, we will always be able to assert a position on the moral and legal acceptability of their use. It does not follow that simply because a technology exists, its use is acceptable.

So what if autonomous weapon systems are developing incrementally?

I want to return to the second assumption insisted upon by Anderson and Waxman, namely that autonomous weapons systems will develop 'incrementally'. What is this assumption meant to do for their argument? Again, from the perspective of technological development, all technologies develop incrementally in some sense. Why would this change the way in which we address their ethical and legal implications? Perhaps Anderson and Waxman are merely trying to disarm the fear that soldiers will be replaced by robots in some great technological leap. As their argument continues, it becomes clearer that what they have in mind is that the transition to autonomous weapon systems will happen in incremental 'baby steps', each of which will be carefully considered and scrutinized. This is a rather inventive inversion of the slippery slope argument. Instead of asserting that these technologies are dangerous because they encourage us to delegate more and more authority to automated systems, eventually resulting in automated systems with the illegitimate but *de facto* authority to target and kill humans, it argues that such systems will be legitimate because each step along the way seems acceptable. They appear to argue that we should accept the end result of this line of reasoning because we were able to reach it through a series of moral adjustments, none of which on its own seemed too awful.

It would make more sense to see this as a slippery slope leading us to a result we believe to be unacceptable. This should lead us to look more carefully for an underlying principle upon which we can stop the perilous slide to an undesirable conclusion. And indeed, there is a principled boundary that we can establish with regard to autonomous weapon systems. That boundary is that for any system capable of initiating lethal force, a human being needs to be meaningfully involved in making the decision of whether or not lethal force will actually be used in each case. And while we can blur this line with various technological systems of shared and supervisory control, we could also design those systems in such ways as to make this line clearer, and to make those decisions better informed.[34]

On the need to establish norms

The conclusions that Anderson and Waxman draw are wrong about the implications of a ban on autonomous weapon systems, but they are correct about the significance of the establishment of norms regarding their use and the need for some constraints:

> The United States must act, however, before international expectations about these technologies harden around the views of those who would impose unrealistic, ineffective or dangerous prohibitions or those who would prefer few or no constraints at all.[35]

What they recognize is that there is a new moral space being opened up by these technologies, and it is not yet settled what the international community will accept as the new norms of warfare in the age of robotics and automation. They are also correct that the US, as both a super power and the leader in developing many of these new technologies, is in a unique position to establish the precedents and norms that will shape the future of armed conflict. More obviously, Anderson and Waxman have not shown how banning autonomous weapon systems is unrealistic, nor have they shown any evidence that such a ban would be ineffective or immoral. Let us consider each of these claims in turn.

How might we make sense of the claim that a ban on autonomous weapon systems would be unrealistic? Is it that such a ban would, in practice, be difficult to implement? All arms control treaties pose challenges in their implementation, and a ban on autonomous weapon systems should not prove exceptionally more or less difficult than others, and therefore is not unrealistic in this sense. Or is the claim that it would be politically difficult to find support for such a ban? In my personal experience, there are a great many individuals, particularly among military officers and policymakers but also among engineers and executives in the defence industry, who would support such a ban. Moreover, it is clear, from my experiences in engaging with the public, that strong moral apprehensions about automated weapons systems are broad-based, as is fear of the potential risks they pose. At the

34 P. Asaro, above note 29, pp. 20–24.
35 K. Anderson and M. C. Waxman, above note 3, p. 2.

very least, a ban is not unrealistic in the sense that it might likely find broad public and official support.

Indeed, the only way we might consider such a ban to be unrealistic is if we accept Anderson and Waxman's unwarranted assumption that these systems are inevitable. If we accept that as a foregone conclusion, then attempting to halt the inevitable does seem unrealistic. But there is nothing inevitable about an emerging technology, the capabilities of which do not yet exist, and the norms surrounding which have not yet been established.

Anderson and Waxman also anticipate an objection to autonomous weapon systems on the basis of a moral principle:

> A second objection is a moral one, and says that it is simply wrong per se to take the human moral agent entirely out of the firing loop. A machine, no matter how good, cannot completely replace the presence of a true moral agent in the form of a human being possessed of a conscience and the faculty of moral judgement (even if flawed in human ways). In that regard, the title of this essay is deliberately provocative in pairing 'robot' and 'soldier', because, on this objection, that is precisely what should never be attempted.
>
> This is a difficult argument to address, since it stops with a moral principle that one either accepts or does not.[36]

The objection they refer to draws upon what is supposed to be a sort of stand-alone principle.[37] Therefore, they suppose that there is no justification for accepting it apart from one's own moral intuitions. I would submit that the arguments presented above in this article have demonstrated that the moral principle for rejecting autonomous weapon systems is in fact implicit within IHL through its various anthropocentric formulations and requirements. Moreover, it is implicit within the very structure of law, the processes of justice, and due process in particular. We require the presence of a human as a legal agent, independent of the moral requirement that they be moral agents.

It is not simply that the decision to kill is a weighty one, though it is. The decision to kill a human can only be legitimate if it is non-arbitrary, and there is no way to guarantee that the use of force is not arbitrary without human control, supervision, and responsibility. It is thus immoral to kill without the involvement of human reason, judgement, and compassion, and it should be illegal.

Conclusion

As a matter of the preservation of human morality, dignity, justice, and law we cannot accept an automated system making the decision to take a human life. And we should respect this by prohibiting autonomous weapon systems. When it comes

36 *Idem*., p. 11.
37 M. Bolton, T. Nash and R. Moyes, above note 11.

to killing, each instance is deserving of human attention and consideration in light of the moral weight inherent in the active taking of a human life.

As technology advances, it gives humanity greater control over the world. With that new control comes increased responsibility. While this seems obvious for technologies that influence human and environmental welfare, it is also true for military technologies. While the development of advanced military technologies does not necessarily imply that they will be, or can be, used more carefully and ethically, that possibility exists. But new capabilities also bring with them a potential to regress in ethics and morality, rather than progress. Ultimately the nature of our moral progress in the conduct of war depends upon our technology in a deeper sense than merely enabling combatants to conduct wars with fewer casualties, and goes beyond the requirements of IHL and IHRL. In choosing the weapons and tactics with which we engage in armed conflict, we are also making a moral choice about the world we wish to live in and fight for, and the legitimate conditions under which we can bring that world into being. In making such choices, we must resist arguments that any end is either so desirable or undesirable that any means of achieving it are acceptable. We must also acknowledge that the means by which we enact change in the world, or resist change, thereby become an aspect of that world. If we truly wish to build a future in which armed conflict is both unnecessary and unacceptable, we must arrive there through a process that raises our moral standards with each new technological innovation, rather than by lowering those standards.

The international community should begin discussions on the formation of a treaty to ban autonomous weapons systems. Insofar as such systems do not yet exist, such a ban would help to focus the development of future military technologies away from these so-called ethical systems and towards the development of systems that can actually improve the ethical conduct of humans in armed conflicts. The critics of such a ban base their criticisms on unsupported claims about the inevitability of these technologies and misleading claims about ethically enhanced technologies. For as long as their potential capabilities remain uncertain, these technologies are emerging in a dynamic field of ethical and legal norms. Though we might like to trust in the promise of more ethical wars through these hypothetical autonomous weapon systems, the reality is that they can also degrade our conceptions and standards of ethical conduct, and distract us from developing the technological enhancement of human moral reasoning by pursuing an improbable technology that threatens to undermine our human rights on a fundamental level. It might also distract us from enhancing and improving IHL and IHRL to deal appropriately and morally with these new technologies.

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

Beyond the Call of Duty: why shouldn't video game players face the same dilemmas as real soldiers?

Ben Clarke, Christian Rouffaer and François Sénéchaud*

Ben Clarke is an associate professor, University of Notre Dame Australia, and former adviser at the Civil Society Relations Unit, International Committee of the Red Cross (ICRC).

Christian Rouffaer is adviser at the Unit for Relations with Armed Forces, Division for the Integration and Promotion of the Law, ICRC.

François Sénéchaud is the head of division for the Integration and Promotion of the Law, ICRC.

Abstract

Video games are influencing users' perceptions about what soldiers are permitted to do during war. They may also be influencing the way combatants actually behave during today's armed conflicts. While highly entertaining escapism for millions of players, some video games create the impression that prohibited acts, such as torture and extrajudicial killing are standard behaviour. The authors argue that further integration of international humanitarian law (IHL) can improve knowledge of the rules of war among millions of players, including aspiring recruits and deployed soldiers. This, in turn, offers the promise of greater respect for IHL on tomorrow's battlefields.

* We would like to thank Helen Durham, Alexandra Boivin, Neil Davidson, Ray Smith, and Vincent Bernard for their valuable input. The views expressed here are those of the authors and do not necessarily reflect the position of the International Committee of the Red Cross.

doi:10.1017/S1816383113000167

Keywords: video games, influence, behaviour, undermining effect, applicability, challenges, messages, obligation, initiative, trivializing.

: : : : : : :

> As I scan the horizon for targets, a river of flames cuts through the night sky; dancing streams of red and white light up the city. I see white phosphorous all around us. This stuff is death to all it touches. Our 155 mm artillery shells, alternating between white phosphorous and high explosive, soften up enemy positions in advance of the assault. In a split second, we will leave the safety of our armoured vehicle and start the bloody work of grunts: searching houses and killing villains. We must push forward. We can't let the terrorists fall back and regroup. We've grabbed a foothold in the city and must exploit it by driving as deep as possible into enemy territory. Our instructions are to take out the likely enemy headquarters, a big house down the street. The success of the whole campaign rests upon our shoulders.
>
> Our squad leader turns to us, gives a few quick orders, and moves to the back gate. I throw a grenade toward the municipal building. When it explodes, smoke and dirt swirl around the street. We fire a few 40 mm M203 rounds for good measure. The explosion leaves a makeshift smoke screen. As we progress, one team member is taken down by sniper fire from a building on our left. It looks like a hotel. I call in a drone strike. Almost immediately its lethal load hits the multistorey building, reducing it to rubble. No need to bother about potential occupants or collateral damage; the entire city, manned only by treacherous terrorists, can be destroyed. Any human our team encounters is a target. Anti-personnel land mines are a good way to secure streets and buildings we have cleared. For four hours in a row, we repeatedly enter houses, killing anyone in our line of sight and grabbing their dog tags as trophies. Enemy wounded, as a rule, try to fight back. Those who don't get a double tap anyway, just like all the rest. After all, there is no surrender option. Only enemy leaders are taken alive: you can't beat intelligence out of dead people. Afterwards, headshots from my M4 Bushmaster – with the silencer I got for reaching 100 kills – are good for my game ranking.[1]

Video games[2] offer players the possibility to 'use' the latest weapons against enemy combatants on contemporary battlefields. Yet as realistic as they may look and sound, these games often portray lawless armed conflicts in which actions are without consequences. This sends negative messages to players about the existence of, and need to respect, humanitarian norms during real armed conflicts. Why can't

1 Fictional account inspired by the authors' experience of video games and an account of the battle of Fallujah in David Bellavia, *House to House – an Epic Memoir of War*, Free Press, New York, 2007.

2 In this article, the term 'video games' is used to describe electronic first person shooter games depicting combat situations – including contemporary battlefields, such as Iraq, Afghanistan, Lebanon, Somalia, and the Levant – where players fire at enemy targets. 'First person shooter games' is the industry's term for electronic games where players fire at enemy targets. As this article is aimed at a broader readership, the term 'video games' is used instead.

players enjoy video games that truly reflect the dilemmas of modern combatants? Can video games be a positive medium of influence to reinforce understanding and respect for the law? Why can't players be rewarded for compliance with the rules governing the use of force as well as the treatment of persons in the hands of the enemy and sanctioned for violating the same?

***

With hundreds of millions of active players (or 'gamers') around the world,[3] the video games industry has become a global phenomenon that transcends social, cultural, geographical, age, and income brackets. While the vast majority of video games do not depict combat situations or indeed any form of violence, those that do represent a highly lucrative, if narrow, segment of the video game market.[4] From Rio de Janeiro to Ramallah, children and adults – including enlisted soldiers and budding recruits – are enthralled by this form of 'militainment' (see figures throughout article).[5]

'Video games and international humanitarian law (IHL)' is a relatively new and fragmented field of enquiry, spanning a range of discourses. There is little in the way of IHL-focused literature on the subject. This article is very much an exploratory piece. Its purpose is to highlight the potential impact of these games on players' perceptions of the normative framework governing the use of force. Our focus is upon first person shooter games depicting combat situations, that is, those games where players fire at enemy targets on contemporary battlefields, such as Iraq, Afghanistan, Lebanon, Somalia, and other contexts in the Levant.[6] As depiction of violence per se is not the issue being addressed in this contribution, video games that portray more fictional scenarios including medieval fantasy or futuristic wars in outer space are beyond the scope of this article. In the first section, we begin by highlighting the potential influence of video games on players' perception about applicable rules in real battlefields. The second section examines the applicability of IHL and international human rights law (IHRL) to contemporary situations portrayed in video games. In the third section, attention turns to challenges posed to

3 One company, Spil Games, claims to have 130 million active monthly users of its online games. It estimates that 510 million people were playing online games in 2010: *SPIL GAMES, 2010 State of Gaming Report*. According to one estimate this is multi-billion dollar industry generated at least $70 billion in 2011. See IDATE, *World Video Game Market Data & Forecasts*, *2011–2015*, 17 January 2012.

4 At the time of publication, the most popular video games were *Call of Duty: Black Ops 2, Madden NFL '12, Halo 4, Assassin's Creed 3, Just Dance 4, NBA 2K13, Borderlands 2, Call of Duty: Modern Warfare 3, Lego Batman 2: DC Super Heroes*, and *FIFA '12*. For current sales figures for the various platforms (games), see '10 best selling videogames in 2012', in *Market Watch,* 10 January 2013, available at: http://www.marketwatch.com/story/10-best-selling-videogames-in-2012-2013-01-10 (last visited January 2013).

5 'Militainment' has been defined as 'war packaged for pleasurable consumption' and 'entertainment with military themes in which the (US) Department of Defense is celebrated'. See Roger Stahl, *Militainment, Inc. – War, Media and Popular Culture*, Routledge, New York, 2009, p. 6, and view 'Militainment, Inc: militarism and pop culture', available at: http://video.google.com/videoplay?docid=-2373519247173568764 (last visited 25 May 2012).

6 Electronic games can be played on different platforms the most common being PCs and consoles. Games played on PCs are commonly known as 'computer games' while those played on consoles are called 'video games'. This article uses the term video games to refer to both.

humanitarian norms by games that are marketed as providing a 'real-life' experience of combat, but actually portray battlefields that are essentially lawless. In the final section, the authors explain the International Committee of the Red Cross's (ICRC) joint initiative with various Red Cross National Societies to work together with the video game industry to encourage innovation for better integration of IHL and IHRL in these games. We note that through this initiative, video games – with their vast reach and capacity for the transfer of knowledge and skills – can become important vectors for the promotion of humanitarian norms.[7]

Influence of video games

Video games and violent behaviour

It is a truism that technology is transforming how wars are fought. In our view, technology is also transforming the way we imagine war. Traditionally, perceptions of war have been shaped by heroic and epic songs, stories, plays, and movies. Today, millions have ready access to increasingly realistic movies and video games crafted with input from ex-military personnel who served on contemporary battlefields.[8] In some cases, the depiction of armed conflict in video games is so realistic that it is difficult to distinguish real war footage from fantasy (Figures 1 and 2).[9] When compared to movies, video games have unprecedented novelty. Players are active participants in simulated warfare. Unlike passive spectators of traditional media such as movies, video game players make decisions to use or refrain from using force. In reaction to this development, 59 per cent of respondents to an Australian government survey stated that video games should be classified differently to other media forms, precisely because the player is invited to participate in video game violence, not just watch violence.[10]

In the same survey, 63 per cent of respondents believed that playing violent computer games results in real life violence. While this widespread belief is revealing, it is not conclusively supported by research. The scientific literature is divided on the influence of video games on human behaviour,

7 The same is true of military training simulators that depict contemporary battlefields. Increasingly, they are used by armed forces to operationalize the laws of armed conflict for military personnel. Given their function, military training simulators are more likely to integrate IHL than commercial video games. However, they also reach a far smaller audience. For these reasons the primary focus of this article is on video games.

8 The increasing realism of video games that depict modern battlefields has drawn attention to commercial-military collaboration in the development of games. See, for instance, 'Documentary – Official Call of Duty Black Ops 2', available at: http://www.youtube.com/watch?feature=player_embeded&v=Gm5PZGb3OyQ (last visited 24 May 2012).

9 What qualifies as a 'realistic video game that portrays armed conflict' is nuanced and somewhat subjective. Some games include realistic looking weapons and battlefield environments but have unrealistic features (e.g., players can come back to life).

10 Australian Government Attorney-General's Department, *Community Attitudes To R18+ Classification Of Computer Games*, Report, November 2010, available at: www.ag.gov.au (last visited 5 April 2012).

Figure 1. This is a real photo-image taken during combat in Fallujah. © Anja Niedringhaus/ Keystone.

Figure 2. In *ArmA II*, players fight in realistic looking environments. This and other scenes closely resemble footage recorded during real military operations. © Bohemia Interactive.

especially when the question is framed: 'Can playing video games lead to violent behaviour?'[11] While there is no compelling evidence to support that proposition, revelations that killers have actually used video games as training tools has kept these issues in the media spotlight.[12]

When it comes to defining the psychological impact of a particular stimulus on an individual, scientific researchers cannot overcome a number of impediments to drawing conclusions that apply to a population as a whole. A range of factors produce differences from one person to another including genetics, the social environment, and the degree of violence within the society of one particular individual. Access to weapons, poverty, and the degree of violence within one's family are believed to be essential factors in the decision to resort to armed violence. Moreover, most scientific research on the causes of violent behaviour is conducted within developed countries where violence is more limited and severely sanctioned. As access to Internet and video games is no longer limited to privileged countries,[13] scientific research conducted in say Nairobi or in the favelas of Rio de Janeiro could yield very different conclusions from existing, often US-based,

11 For an illustration of the scientific debate: Anderson *et al*, assert a causal link between violent games and violent behaviour: Craig A. Anderson, Akiko Shibuya, Nobuko Ihori, Edward L. Swing, Brad J. Bushman, Akira Sakamoto, Hannah R. Rothstein and Muniba Saleem, 'Violent video game effect on aggression, empathy and prosocial behaviour in eastern and western countries: a meta-analytic review', in *Psychological Bulletin*, Vol. 136, No. 2, pp. 151–173. For Ferguson the link is not proven and attention should be focused elsewhere (e.g., on poverty and domestic violence). See Christopher J. Ferguson, 'Media violence effects: confirmed truth or just another X-file?', in *Journal of Forensic Psychology*, Vol. 9, No. 2, April–June 2009, pp. 103–126. This is also the conclusion of the Swedish Media Council, *Summary of Violent Computer Games and Aggression – An Overview of the Research 2000–2011*, Swedish Media Council, Stockholm, 2012, available at: http://www.statensmedierad.se/upload/_pdf/Summery_Violent_Computer_Games.pdf (last visited 20 December 2012), and *Brown, Governor of California, et al.* v. *Entertainment Merchants Association et al.*, Certiorari to the United States Court of Appeals for the Ninth Circuit, No. 08–1448. Argued 2 November 2010 – Decided 27 June 2011 (hereinafter '*Brown*') where the majority of the US Supreme Court noted that: 'Psychological studies purporting to show a connection between exposure to violent video games and harmful effects on children do not prove that such exposure causes minors to act aggressively. Any demonstrated effects are both small and indistinguishable from effects produced by other media' (Scalia, J., p. 13, who delivered the opinion of the Court, in which Kennedy, Ginsburg, Sotomayor, and Kagan, JJ., joined. Alito, J., filed an opinion concurring in the judgment, in which Roberts, C. J., joined. Thomas, J., and Breyer, J., filed dissenting opinions.)

12 Tragic events including mass killings by gunmen at Columbine, Virginia Tech, and Sandy Hook have heightened public concern. Like Norwegian mass murderer Anders Breivik, several US perpetrators regularly played *Call of Duty*. Police observations regarding similarities between Sandy Hook gunman Adam Lanza's modus operandi and methods used in a video game he frequently played are particularly revealing. See Dave Altimari and Jon Lender, 'Sandy Hook shooter Adam Lanza wore earplugs', in *Hartford Courant*, 6 January 2013, available at: http://articles.courant.com/2013-01-06/news/hc-sandy-hook-lanza-earplugs-20130106_1_police-cars-lauren-rousseau-newtown (last visited 10 January 2013).

13 In 2008 an estimated 31,68 million people, worldwide, played online video games, out of which an estimated 3 million played first person shooter games. These figures do not take into account those people who played either on unconnected computers, PlayStations or cell phones. In the Middle East, in 2010, 64 million people played online video games or on PlayStations. In 2012 there are an estimated 211.5 million video-games players in the US. See 'Mobile gamers now represent the largest gamer segment', in *NPD*, 5 September 2012, available at: https://www.npd.com/wps/portal/npd/us/news/press-releases/pr_120905/ (last visited 20 October 2012). In Turkey, in 2012, an estimated 21.8 million people played video games on computers, smartphones, and game consoles. See 'Infographic 2012', in *NewZoo*, 21 June 2012, available at: http://www.newzoo.com/infographics/infographic-turkey/ (last visited 20 October 2012).

research.[14] In any case, while researchers have not established a causal link between violent games and violent behaviour, they have not excluded such a link.

Video games, training, and skills acquisition

There is little doubt that video games represent an efficient medium for the transfer of knowledge and skills. According to a recent French language survey,[15] more than 50 per cent of players claimed to play between one and four hours per day and over 90 per cent had played games depicting graphic armed violence. Repetition of actions is essential to the acquisition of automatism. Recognized by military leaders since antiquity, this technique is institutionalized in military training, and commonly known as 'the drill'. While playing for hours, regularly repeating the same actions and scenarios, video game players focus on the objective to be attained. Methods used are simply a means to achieving the goal. Inevitably, players learn from their own actions as well as from images displayed on the screen.

When performing as expected by the video game scenario or script, players are rewarded symbolically with a bonus, a medal, or improved equipment or weaponry, or by moving to the next stage of the game. Such rewards, combined with hormones produced by the brain, provide a sense of satisfaction and fulfilment for actions performed and skills learned.[16] Arguably, a player regularly exposed to video game scenes of torture and perhaps compelled by the script to act out torture[17] (to proceed to the next stage) and then rewarded for doing so will not necessarily commit acts of torture in real life. However, such a person may find himself or herself more easily inclined to regard torture as an acceptable behaviour. A study, conducted by the American Red Cross, while not mentioning video games, offers important insights into what Americans think about certain conduct frequently depicted in video games, including torture.[18] Of the youth surveyed, 59 per cent considered the torture of captured enemy soldiers or fighters in order to

14 In the US alone there have been more than 200 studies into violence in the media. Over the last eighty years these studies have gradually shifted from cinema, to television, and now concentrate on video games.

15 Gaël Humbert-Droz, 'Les jeux vidéos et le droit international', 2012. This survey was posted on the following forums: jeuxvideo.com, Forum FantabobShow, Forum DpStream : Forum BF-France (battlefield France). The survey is no longer available online (copy on file with the authors).

16 See, for instance, Douglas A. Gentile, 'Video games affect the brain – for better and worse', in *the Dana Foundation*, 23 July 2009, available at: http://www.dana.org/news/cerebrum/detail.aspx?id=22800 (last visited 10 February 2012).

17 By way of example, torture scenes appear in *Call of Duty: World at War*. See 'Call of Duty: Modern Warfare 2', in *Wikia*, available at: http://callofduty.wikia.com/wiki/Call_of_Duty:_Modern_Warfare_2 (last visited 10 October 2012). In *Call of Duty: Black Ops*, the player must take part in an act of torture (they must give a command for the hero to hit in the face a detainee in whose mouth shards of glass were previously introduced). In *Call of Duty: Modern Warfare 3*, the superior of the player tortures a Somali commander before shooting a bullet in his head (Figure 4). While the presence of torture in the narrative of these games certainly leaves no one indifferent, the rationale for its inclusion is unclear.

18 More than two-fifths of youth (41%) believe there are times when it is acceptable for the enemy to torture captured American prisoners, while only 30% of adults agree. More than half of youth (56%) believe that there are times when it is acceptable to kill enemy prisoners in retaliation if the enemy has been killing American prisoners, while only 29% of adults agree. Brad A. Gutierrez, Sarah DeCristofaro and Michael Woods, 'What Americans think of international humanitarian law', in *International Review of the Red Cross*, Vol. 93, No. 884, December 2011, pp. 1009–1034.

extract important military information as acceptable (compared to 51 per cent of adults). Only 45 per cent and 40 per cent respectively said this conduct was never acceptable.

The utility of video games and virtual environments for training and skills acquisition has been recognized by armed forces, leading to commercial-military collaboration in the development of games. Collaboration between the video game industry and the military is not new.[19] Interaction flows in two directions and takes several forms. Commercial war game developers advise the armed forces on how to make their recruitment games more entertaining, while serving or former military personnel add realism to stories and scenes in commercial games.[20] Meanwhile, footage from real armed conflicts is adapted for use in both battlefield training software and commercial video games. Military interest in video games is not difficult to fathom. According to one study, US military personnel and potential recruits play video games at a higher rate than the general population.[21] A US Navy review of the effectiveness of instructional games concluded that, for various different tasks and diverse learning groups, some games could provide effective learning in areas such as mathematics, attitudes, electronics, and economics.[22] Computer simulation programmes have also been developed to assist veterans to reintegrate into society[23] and help trauma victims.[24] Another instance of the use of video games as a medium of influence is provided by the US Army's most powerful recruitment tool: a multiplayer[25] video game. In *America's Army*, players

19 For a brief history of how 'virtual worlds of war became a mutual enterprise uniting the media and military industries', see Robin Andersen and Marin Kurti, 'From *America's Army* to *Call of Duty*: doing battle with the military entertainment complex', in *Democratic Communique*, Vol. 23, No. 1, 2009, p. 45, available at: http://www.democraticcommunications.org/communique/issues/Fall2009/andersen.pdf (last visited 20 February 2012). See also, Tony Fortin, 'Jeux vidéo et monde militaire, un couple inséparable?', in *Rue89*, 22 September 2012, available at: http://www.rue89.com/2012/09/22/jeux-video-et-monde-militaire-un-couple-inseparable-235526 (last visited 20 October 2012).

20 For example, in 2002, Bohemia Interactive, creators of the video game *ARMA II*, developed a battlefield simulation system for the US armed forces. *Virtual Battlespace* (*VBS*) 1 and 2 are now used by armed forces including the US Marine Corps (and several other branches of the US armed forces), the British, Australian, New Zealand, and Canadian armed forces, and NATO. See also, 'US Army's new virtual simulation training system', in *Defence Talk*, 30 May 2011, available at: http://www.defencetalk.com/army-virtual-simulation-training-system-34543/ (last visited 20 October 2012).

21 US military research suggests that 75% of male staff enlisted in the US military may play video games at least once a week, compared to 40% of the general US population. B. W. Knerr, 'Virtual media for military applications', Paper 21, *Current Issues in the Use of Virtual Simulations for Dismounted Soldier Training Data*, 2006. The study does not specify the type of game played (e.g., first person shooter or role-playing game).

22 Robert T. Hayes, 'The effectiveness of instructional games: a literature review and discussion', Naval Air Warfare Center Training Systems Division, Orlando, 2005, p. 6, available at: http://www.stottlerhenke.com/projects/matisse/background_docs/Instr_Game_ReviewTr_2.005.pdf (last visited 10 January 2012).

23 'US war woe: suicide kills more soldiers than combat', in *RT*, 23 December 2011, available at: http://www.rt.com/news/us-soldiers-suicide-combat-487/ (last visited 20 May 2012).

24 See Laurin Biron, 'Virtual reality helps service members deal with PTSD', 11 June 2012, available at: http://www.defensenews.com/article/20120611/TSJ01/306110003/Virtual-Reality-Helps-Service-Members-Deal-PTSD (last visited 20 June 2012). See generally, Jane McGonigal, *Reality Is Broken: Why Games Make Us Better and How They Can Change the World*, Penguin Press, New York, 2011 (this post-doctoral work assesses how to harness the power of games to solve real-world problems).

25 Multiplayer games are set in an open battlefield. Dozens of people connect to the Internet compete to capture the enemy flag or eliminate other players.

engage – together with others connected on the Internet – in imaginary military operations in mostly urban settings that resemble combat conditions in Iraq and Afghanistan. Massachusetts Institute of Technology (MIT) researchers argue that this free online game is a more effective recruitment tool than all other forms of US Army advertising combined.[26] In addition to being a useful vector for communicating information of clear interest to potential recruits (for example, equipment, salaries, and career opportunities), the game is a tool for inculcating military values.[27]

Resorting to video games as a medium of influence is not limited to the US or Western world armed forces. *Under Siege* (*Tahta – al Hisar*),[28] a video game developed and produced in Damascus, Syria, departs from the familiar script of American soldiers as the heroes doing battle in Muslim countries. Set during the Second Intifada and designed for Arab youngsters, *Under Siege* offers a Middle Eastern view of that conflict. Players get to assume the role of a young Palestinian facing Israeli occupation. Hezbollah's video game *Special Forces 2 – Tale of the Truthful Pledge*, a follow up to *Special Force* (2003), adopts a similar approach. The second edition depicts armed conflict between Israel and Hezbollah based on key phases of the 2006 armed conflict.[29]

Another, albeit indirect, form of interaction between the military and the video game 'sphere' is to be observed through the new generation of unmanned aerial vehicle (or drone) pilots who bring years of video-gaming experience to their new role of conducting combat operations.[30] This has sparked debate about whether such experience shapes attitudes and behaviour. The question of whether drone pilots have a 'PlayStation mentality' has generated heated debate within military circles. Concerns have been voiced by senior military officials about video games shaping perceptions about what is acceptable behaviour during war, including the perceptions of experienced video gamers recruited to operate armed drones from remote locations far from the battlefield.[31] This issue deserves further examination by researchers independent of government and military forces.

The then UN Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions Philip Alston, frames the issue in the following way:

> Young military personnel raised on a diet of video games now kill real people remotely using joysticks. Far removed from the human consequences of their

26 Jeremy Hsu, 'For the US military, video games get serious', in *Live Science*, 19 August 2010, available at: http://www.livescience.com/10022-military-video-games.html (last visited 15 June 2012).

27 One example is the notion of hero: biographies of 'real heroes' in the US army can be found on the *America's Army* website, available at: http://www.americasarmy.com/realheroes/ (last visited 24 May 2012).

28 Kim Ghattas, 'Syria launches Arab war game', in *BBC News*, 31 May 2002, available at: http://news.bbc.co.uk/2/hi/middle_east/2019677.stm (last visited 15 June 2012).

29 Tom Perry, 'Hezbollah brings Israel war to computer screen', in *Reuters*, 16 August 2007, available at: http://www.reuters.com/article/2007/08/16/us-lebanon-hezbollah-game-idUSL1662429320070816 (last visited 10 January 2012).

30 Peter W. Singer, 'Meet the Sims . . . and shoot them', in *Foreign Policy*, March 2010, available at: http://www.foreignpolicy.com/articles/2010/02/22/meet_the_sims_and_shoot_them (last visited 24 May 2012).

31 Air Marshall Brian Burridge, 'Post-modern warfighting with unmanned vehicle systems: esoteric chimera or essential capability?', in *RUSI Journal*, Vol. 150, No. 5, October 2005, pp. 20–23.

> actions, how will this generation of fighters value the right to life? How will commanders and policymakers keep themselves immune from the deceptively antiseptic nature of drone killings? Will killing be a more attractive option than capture? Will the standards for intelligence-gathering to justify a killing slip? Will the number of acceptable 'collateral' civilian deaths increase?[32]

Video games and the factors influencing the behaviour of combatants

On the issue of video games and their potential influence on behaviour, it is instructive to compare the mechanisms that shape the behaviour of combatants in real life and those at play within video games. Through empirical research and a review of the literature, the ICRC has identified various factors that are crucial in conditioning the behaviour of combatants in armed conflicts. The goal of a 2004 study[33] was to identify the causes of violations of IHL. It focused mainly on psycho-sociological factors universally present in any group of armed combatants taking part in a war, such as the influence of the group, integration within a hierarchy, and moral disengagement.[34] Interestingly (or disturbingly), most of these factors may also be identified in video games. With respect to behaviour of combatants, the study found that:

> Combatants are subject to group conformity phenomena such as depersonalization, loss of independence and a high degree of conformity. This is a situation that favours the dilution of the individual responsibility of the combatant within the collective responsibility of his combat unit. . . . Combatants are also subject to a process of shifting individual responsibility from themselves to their superior(s) in the chain of command. While violations of IHL may sometimes stem from orders given by such an authority, they seem more frequently to be connected with a lack of any specific orders not to violate the law or an implicit authorization to behave in a reprehensible manner. . . . Combatants who have taken part in hostilities and been subjected to humiliation and trauma are led, in the short term, to perpetrate violations of IHL. . . . The gulf observed between the acknowledgement and application of humanitarian norms derives from a series of mechanisms leading to the moral disengagement of the combatant and to the perpetration of violations of IHL. The moral disengagement of

32 Philip Alston and Hina Shamsi, 'A killer above the law', in *The Guardian*, 2 August 2010, available at: http://www.guardian.co.uk/commentisfree/2010/feb/08/afghanistan-drones-defence-killing (last visited 1 August 2012).

33 Daniel Muñoz-Rojas and Jean-Jacques Frésard, 'The roots of behaviour in war – understanding and preventing IHL violations, in *International Review of the Red Cross*, Vol. 86, No. 853, March 2004, pp. 169–188 (hereinafter 'the study').

34 'Moral disengagement is a complex process and malicious acts are always the product of interactions between personal, social and environmental influences'. *Ibid.*, p. 197. 'Moral disengagement is not only a gradual process but also one that determines behaviour which draws from past actions the force needed to sustain future actions'. *Ibid.*, p. 199.

combatants is effected mainly by having recourse (1) to justifications of violations,[35] and (2) to the dehumanizing of the enemy.[36]

Several parallels may be drawn between the conclusions of this study and video games that portray contemporary battlefields. Out of the five causes of violations identified in the study, at least four are mirrored in video games. Namely, the encouragement to crime that is part of the nature of war, the definition of war aims, reasons of opportunity, and psycho-sociological reasons. It goes without saying that reasons linked to the individual (the fifth identified cause of violations) may not be generalized here.

The study identified encouragement to crime[37] as part of the nature of war. In video games it flows from perceptions that battlefields are places devoid of civilians or those *hors de combat*. Consequently, players are left under the impression that the whole battlefield is an open shooting range where no precautions are to be taken. In the view of the authors, the decision of video game companies to remove civilians from their products fuels the same perception: anything alive is a foe and killing is the only option – there are no limits to the use of force. This impression is reinforced by the example sometimes set by the behaviour of other characters in the video games. For instance, when a squad leader in a video game engages in torture or extrajudicial killing, this provides the signal to players that such behaviour is implicitly authorized.[38]

The definition of war aims (or campaign objectives) of video games tends to justify the results, whatever the methods. As in real armed conflict, the enemy is commonly demonized and dehumanized in video games, justifying their killing. The enemy's failure to respect the law is also presented as a justification for players using any method of warfare at their disposal to fulfil their mission.

In real armed conflicts many combatants break the rules simply because war is the ultimate experience and they are given the opportunity to do so. Such reasons of opportunity are reflected by the enjoyment of transgressing rules. This is at the very centre of the experience of many types of video games, including many that depict contemporary battlefields. As noted by some video games developers,

35 Combatants resort to different justifications or a combination thereof, such as declaring oneself not as a torturer but as a victim; arguing that circumstances render some reprehensible behaviour not only admissible but also necessary; invoking violations by the enemy and sometime blaming the victims themselves; or denying, minimizing, or ignoring the effects of their actions through the use of euphemisms to refer to their operations and their consequences. *Ibid.*, pp. 198–200.

36 'The humanity of the other side is denied by attributing to the enemy contemptible character traits or intentions . . .', sometimes equating it with vermin or viruses to be eradicated. 'Combatants thus find it easier not only to attack but also to rationalize the most extreme kinds of behaviour and to convince themselves that they are justified and necessary'. *Ibid.*, p. 199

37 *Ibid.*, p. 189.

38 'Ordinary men submit willingly to an authority when they believe that it is legitimate; they then perceive themselves as its agents . . . This principle . . . is further reinforced when it is a question of combatants placed within a military hierarchy, a framework generally more constraining than any civilian authority . . . Although, under these conditions, the individual commits acts which seem to violate the dictates of his conscience, it would be wrong to conclude that his moral sense has disappeared. The fact is that it has radically changed focus. The person concerned no longer makes value judgements about his actions. What concerns him now is to show himself worthy of what the authority expects of him'. *Ibid.*, pp. 194–195.

players tend to shoot civilians in games simply because they can. For both the combatants and the players, the sense of opportunity is reinforced by a feeling of impunity. In most video games, violations are not followed by sanctions.

Finally, as in real armed conflicts, psycho-sociological reasons such as obedience to authority, group conformity, as well as moral disengagement are all embodied within the limited freedom of decision-making offered to the player. For instance, in one sequence in *Call of Duty: Black Ops*, the player must watch his or her own character introduce shards of glass into the mouth of a captured enemy. Immediately afterwards the player is requested and compelled to give a command to the computer or play station for the hero to hit the detainee in the face. With no other alternative than to obey or quit the game, the player is left to construct his or her own justification for this act of torture in order to distance himself from the facts and continue with his or her life. This mechanism is known all too well to numerous combatants in real armed conflicts.

Applicability of IHL and IHRL to video games

A plethora of legal norms are relevant to video games. Before addressing IHL, it is important to note that players, game designers, and distributors can point to a range of protections guaranteed under IHRL that are relevant to their respective activities. These protections flow from freedom of expression,[39] the right to property,[40] the right to privacy and family life,[41] and the right to play.[42] Freedom of expression, for instance, has been successfully invoked on numerous occasions in US courts to uphold the legality of video and computer games that depict violence, including torture and summary execution of captives.[43] However, this right has its

39 According to Article 19, International Covenant on Civil and Political Rights, entered into force on 23 March 1976 (adopted on 16 December 1966) (hereinafter 'ICCPR'), 'everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice'. For similar guarantees under international and regional instruments, see Article 19 of the Universal Declaration of Human Rights, Article 10 of the European Convention for the Protection of Human Rights, Article 9 of the African Charter on Human and Peoples' Rights, Article 10 of the European Convention on Human Rights and Article 13 of the American Convention on Human Rights.

40 The right to property is found in Article 17 of the Universal Declaration of Human Rights; Article 1 of Protocol I to the European Convention for the Protection of Human Rights; Article 21 of the American Convention on Human Rights; and most explicitly in Article 14 of the African Charter on Human and Peoples' Rights (ACHPR).

41 Article 17 of the ICCPR guarantees the right to protection from unreasonable interference by the state with respect to how computers and the Internet are used in private life.

42 Articles 1 and 31 of the Convention on the Rights of the Child, entered into force on 2 September 1990 (adopted on 20 November 1989).

43 By way of example, attempts to persuade US courts to ban or impose restrictions on games that depict violence rarely succeed. The outcome usually rests on whether games fall within exemptions to freedom of speech. See *American Amusement Machine Association* v. *Kendrick*, CA7 2001, 244. F. 3d 572, 577 (video games are protected on free speech grounds: no compelling justification was offered for the restriction sought); *Benoit* v. *Nintendo of America, Inc.* 2001 Lsa. Dist. Ct. (even if the death of a child during epileptic seizures was caused by exposure to violence in *Mortal Kombat*, the speech in the video game was protected

limits.[44] Lawmakers in various countries have relied upon these limits to ban games that depict extreme physical violence, sexual violence, and other content deemed offensive. The fact that specific provisions of IHRL,[45] copyright and intellectual property law,[46] and domestic law are the main sources of law applicable to the design, sale, and use of video games[47] is uncontroversial and not central to the present article. Of more interest for present purposes is the issue of the applicability of the rules on the use of force and the treatment of persons in the hands of the enemy, as contained within IHL and IHRL, to virtual battlefields created by the militainment industry.

It goes without saying that playing video games falls within the realm of fantasy. It does not involve participation in a real armed conflict. The same is true of use of battlefield simulation technology for military training purposes. Nonetheless, two questions need answers. First of all, do IHL and IHRL rules apply to the situations portrayed within video games? And second, do states have any particular obligation to ensure that the content of video games complies with the rules on the use of force and the treatment of persons in the hands of the enemy?

Any operation on a battlefield takes place within a legal framework shaped by international law (IHL and IHRL) and national legislation. Even though video games are only virtual it is argued here that, for the sake of realism, IHL and IHRL rules on the use of force should be applied to scenes in video games that portray realistic battlefields (in the same way that the laws of physics are applied). Incidentally, video games are not the only context where this legal framework can

unless it was an 'incitement to violence', which it was not); *Video Software Dealers Association* v. *Schwarzenegger*, Appeals Court upheld 2005 District Court 2009 US CA 9th Cir. (legislation restricting sale of violent video games to minors was unconstitutional. For the Supreme Court appeal, see *Brown*, above note 11); *Entertainment Software Association* v. *Granholm* 2005 Mich. Dist. Ct. (violent game protected as free speech, insufficient evidence of harm); and *Entertainment Software Association; Entertainment Merchants Association* v. *Minnesota* 2008 US CA 8th Cir. (injunction granted against law banning the sale or rental of violent video games to minors: freedom of speech and absence of proof of harm were decisive).

44 Freedom of expression can be limited under domestic law to protect the rights and reputations of others, national security, public order, public health, or morals. See Article 19(3) ICCPR.

45 In addition to the treaties mentioned above, others of relevance to video games include: the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, entered into force on 26 June 1987 (adopted on 10 December 1984) (hereinafter 'CAT'), the Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict, entered into force on 12 February 2002 (adopted on 25 May 2000, whether this Protocol is considered as part of IHL or of IHRL is a matter of debate), and the Convention on the Elimination of All Forms of Discrimination against Women, entered into force on 3 September 1981 (adopted on 18 December 1979).

46 Aside from games made available for free by their creators, video-game software is usually protected by copyright laws, international copyright treaties, and other treaties, and intellectual property laws. International agreements on copyright include the Berne Convention for the Protection of Literary and Artistic Works, 1886; Universal Copyright Convention, 1952; WIPO Copyright Treaty, 1996; and The World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), 1994.

47 Domestic legislation can apply to various activities associated with video games. Domestic copyright, property, privacy, and criminal laws (e.g., offences involving inciting racial hatred, providing support for a terrorist organization, etc.) may regulate the creation, distribution, use, and enjoyment of video games. On 'counselling' a criminal offence through video games, see *R.* v. *Hamilton*, Supreme Court of Canada, 29 July 2005, 2 S.C.R. 432, 2005 SCC 47.

shape a situation even though no armed conflict is actually in progress. Another important example is military training and planning. Whenever military commanders train their personnel, or plan operations with their staff, they must take into account the relevant law. They are certainly not expected to wait for the operation to be carried out before factoring in the law.

Whether IHL or IHRL or both are relevant to the situation portrayed in a video game depends upon whether the game depicts a situation of armed conflict. Each game must be examined individually. As IHL only applies during armed conflict, it has no relevance if what is portrayed in a video game is internal tensions, such as riots or protests, falling below the threshold of armed conflict. In these situations, the law enforcement regime,[48] which falls within IHRL, prescribes applicable rules on the use of force, firearms, arrest, detention, search and seizure during law enforcement operations.[49] For example, IHRL provides that firearms may not be used against a person, unless the person in question poses an imminent threat to life and there is no possible alternative.[50] Where the situation portrayed reaches the threshold of armed conflict, both IHL and IHRL are relevant. IHL contains the rules that combatants must follow when planning and conducting military operations (for example, rules on distinction, proportionality, and precautions). The conduct of hostilities regime, which falls within IHL,[51] allows for the killing of legitimate targets.[52] Where it is unclear whether the setting of the video game reaches the threshold of an armed conflict[53] – and therefore whether IHL applies – IHRL continues to be applicable, including the law enforcement

48 The law enforcement regime (IHRL) is the set of rules regulating the resort to force by state authorities in order to maintain or restore public security, law, and order.

49 These rules are found in treaties (e.g., ICCPR; International Convention on the Elimination of All Forms of Racial Discrimination; Convention on the Rights of the Child) and non-binding instruments (e.g., Standard Minimum Rules for the Treatment of Prisoners; Code of Conduct for Law Enforcement Officials; Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power; Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment; Basic Principles for the Treatment of Prisoners; Basic Principles on the Use of Force and Firearms by Law Enforcement Officials; Declaration on the Elimination of Violence against Women).

50 Basic Principles on the Use of Force and Firearms by Law Enforcement Officials, adopted by the eighth United Nations Congress on the prevention of crime and the treatment of offenders, Havana, Cuba, 27 August to 7 September 1990, in particular, provisions 5, 9 and 10.

51 Frida Castillo notes that: 'To define which IHL apply in a given situation, it is necessary to check what instruments were ratified by the state in question. While the 1949 Geneva Conventions were ratified universally, there are other IHL treaties, such as Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non International Armed Conflicts of 8 June 1977 (AP II), which have not been ratified by all states. So here too, it is necessary to verify, whether the states involved in the conflict have ratified the relevant instruments. Rules considered to be customary law on the other hand, apply to all states.' Report by Frida Castillo, *Playing by the Rules: Applying International Humanitarian Law to Video and Computer Games*, TRIAL, Pro Juventute, Geneva, October 2009, p. 3, footnote 1.

52 Combatants and civilians if and for such time as they directly participate in hostilities. See AP I, Articles 48 and 51(3), and Rules 1 and 6 of the ICRC Customary International Humanitarian Law Study. ICRC, *Customary International Humanitarian Law*, Vol. I: rules, Jean-Marie Henckaerts and Louise Doswald-Beck (eds), Cambridge University Press, Cambridge, 2005 ('the ICRC Customary Law Study').

53 While any resort to armed force between two states constitutes an international armed conflict, in order for the threshold of non-international armed conflict to be reached, there must be 'protracted armed violence' involving a sufficient intensity of the violence and level of organisation of the parties. For the intensity requirement, relevant factors cited in case law include: the number, duration, and intensity of

regime referred to above, as well as the prohibition in particular of torture, arbitrary deprivation of life, and cruel and degrading treatment.[54]

Looking at the second question, that is, whether states have an obligation to ensure video game content complies with the rules on the use of force, consider the following hypothetical example. A video game enables players to commit acts of torture and other grave breaches or serious violations of IHL in a virtual armed conflict. Players are not informed that such acts are prohibited. Sometimes players are even rewarded for acting out such behaviour in the game. For the sake of simplicity, let us put the provisions of the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment to one side. Does the game engage the IHL treaty obligations of states to respect and ensure respect[55] and to disseminate[56] IHL as widely as possible?[57] It is uncontroversial to note that states, at the very least, must ensure that their military training tools (including video games used either for recruitment or training purposes) do not permit or encourage any unlawful behaviour without proper sanctions. In the best case scenario, in fulfilment of the state's obligations, military training tools should fully integrate applicable rules on the use of force, that is, these tools should enable military personnel to respect, and train in the respect of, the law.[58] State obligations to 'respect and to ensure respect' for IHL and disseminate IHL as widely as possible and to comply

individual confrontations; the types of weapons used; the number of casualties; the extent of material destruction. See, inter alia, International Criminal Tribunal for the former Yugoslavia (ICTY), *Prosecutor* v. *Ramush Haradinaj, Idriz Belaj, Lahi Brahimaj*, Case No. IT-04-84-T, Judgement (Trial Chamber I), 3 April 2008, para. 49. Indicative factors for the organisation requirement include: the existence of a command structure and disciplinary rules; headquarters; the fact that the group controls a certain territory; the ability to plan, coordinate, and carry out military operations. See, *inter alia*, ICTY, *Ibid*., para. 60.

54 IHL and IHRL contain common prohibitions that must be respected at all times during armed conflict. Examples include the prohibitions against discrimination, summary execution, rape, torture, and cruel and degrading treatment. Both legal regimes also include provisions for the protection of women and children; prescribe basic rights for persons subject to a criminal justice process; and regulate aspects of the right to food and health.

55 Common Article 1 of the four Geneva Conventions of 1949; Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Geneva, 12 August 1949 (hereinafter 'GCI'); Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea. Geneva, 12 August 1949 (hereinafter 'GCII'); Convention Relative to the Treatment of Prisoners of War, Geneva, 12 August 1949 (hereinafter 'GCIII'); Convention Relative to the Protection of Civilian Persons in Time of War, Geneva, 12 August 1949 (hereinafter 'GCIV'). See also, Rule 139 of the ICRC Customary Law Study states that: 'Each party to the conflict must respect and ensure respect for international humanitarian law by its armed forces and other persons or groups acting in fact on its instructions, or under its direction or control'.

56 GCI Art. 47, GCII Art. 48, GCIII Art. 127, and GCIV Art. 144 all provide: 'The High Contracting Parties undertake, in time of peace as in time of war, to disseminate the text of the present Convention as widely as possible in their respective countries and, in particular, to include the study thereof [if possible] in their programmes of … civilian instruction, so that the principles thereof may become known to the entire population'. See also, GCIII, Arts 39 and 41; GCIV, Art. 99; AP I, Art.83; AP II, Art. 19.

57 On the obligation of continuous dissemination, see Claude Pilloud, Yves Sandoz and Bruno Zimmermann (eds), *Commentary to Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977*, ICRC, 1987 (Commentary to Article 80), p. 929, para. 3290.

58 Detailed study of relevant state practice on 'how far these obligations extend' in the context of training tools and 'what are the consequences of failure to fulfil them' exceeds the word constraints of this article. Comprehensive research on these important issues would be useful.

with their treaty obligations[59] are very general and apply at all times.[60] While these rules should, as a matter of logic, apply to commercial video games sold or distributed on the sovereign territory of states, the practice of states indicates otherwise.

To conclude this section, it is important to note that questions about whether States have an obligation to ensure that the rules on the use of force, and the treatment of persons in the hands of the enemy are properly integrated into video games are not just theoretical. Depictions of violations of the law are not uncommon in video games. A 2009 Swiss study of popular video games[61] identified frequently depicted violations of IHL. They included: violations of the principles of distinction and proportionality; extensive destruction of civilian property and/or injury or deaths of civilians without military necessity; and intentionally directing attacks against civilians or civilian objects, including religious buildings.[62] The study found that cruel, inhuman, or degrading treatment or torture was most often depicted in video games in the context of interrogation.[63]

The same study found that direct attacks against civilians not directly participating in hostilities were frequently depicted.[64] The victims – mostly hostages or civilians present in a village – were not mere incidental casualties: they were directly targeted. In only one game was this conduct punished.[65] Indeed, failure to comply with the principle of distinction occurred in various games. One instance is the use of munitions, including tank shells and cluster munitions[66] that are indiscriminate in their effects[67] when deployed in densely populated areas. In *Medal of Honour Airborne*, weapons that do not discriminate between combatants and civilians on the ground are deployed in airborne operations in urban areas.[68] Several games also allowed players to shoot injured soldiers who are *hors de combat* or watch others do so.[69] Many produce inconsistent consequences when players target

59 These provisions are based on the customary rule *pacta sunt servanda* as enshrined in Article 26, of the *Vienna Convention on the Law* of *Treaties*, 23 *May 1969*, 1155 *UNTS* 331.

60 According to the Commentary of Article 1 of GCI, p. 26, 'if it is to keep its solemn engagements, the State must of necessity prepare in advance, that is to say in peacetime, the legal, material or other means of loyal enforcement of the Convention as and when the occasion arises'. See also, Commentary AP I, p. 41; Commentary GCIV, p. 16; Commentary GCIII, p. 18; Commentary GCII, p. 25. According to Art. 1(1) of Protocol Additional I to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 UNTS 3 (entered into force 7 December 1978) (hereinafter 'AP I'), such respect is required 'in all circumstances'.

61 F. Castillo, above note 51.

62 In one game only, *Call of Duty 4 (Modern Warfare)*, attacking a church resulted in termination of the mission (game over). Attacking mosques never triggered this outcome. *Ibid*., p. 24.

63 In many cases, the interrogation ends with extrajudicial execution. *Ibid*., p. 42.

64 *Ibid*., p. 42.

65 *Tom Clancy Rainbow 6 Vegas.* See *ibid*., p. 37.

66 Examples include *World in Conflict* and *Frontlines: Fuel of War*. See *ibid*., pp. 30–31. The Convention on Cluster Munitions of May 2008 (open for signature since 3 December 2008) prohibits the use of cluster munitions by states parties. However, their use in circumstances where civilians and combatants are indiscriminately targeted is always prohibited.

67 For the applicable law see The Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects (entered into force 2 December 1983) 1342 UNTS 137.

68 F. Castillo, above note 51, pp. 34 and 42.

69 *Ibid*., pp.15–16, 42. Relevant games include: *Call of Duty 5 (World at War), Call of Duty: Modern Warfare 3, ARMA II, Call of Duty: Modern Warfare 2, Call of Duty: Black Ops*. See also, *24, The Game*.

civilians or engage in other conduct that would constitute violations in a real armed conflict.[70]

The authors of the present article have identified various other examples in video games of conduct that could constitute violations in a real armed conflict. They include: firing on medical units bearing the Red Cross, Red Crescent, or Red Crystal protective emblem or misuse of that emblem; destruction of civilian objects which appears to be disproportionate; use of anti-personnel landmines; removing identity discs from dead enemy combatants as trophies; use of heavy weapons in densely populated areas without regard for the rules on precautions in attack; and attacks on civilian objects that may involve the death of innumerable unseen civilians.[71] The last two problems are illustrated in the video game *Battlefield 3*. In one scene, an entire floor of a multistorey hotel is destroyed in order to kill a single sniper.

Challenges to humanitarian norms

Simply playing a video game does not give rise to violations of IHL or IHRL by the player. At the risk of stating the obvious, a player does not commit a criminal act by pressing a button to enable a character in a video game to perform torture or summary execution: video games are fantasy. Furthermore, there is neither a need nor a way to take any legal action against gamers in such circumstances. Armed conflicts are, by definition, violent environments in which participants or combatants may apply a certain degree of force to compel the enemy to surrender. The depictions of violence in video games, per se, are therefore not the issue. However, in our view, video games pose two important challenges to humanitarian norms. The first is their tendency to trivialize violations of the law. No less important is their potential undermining effect on perceptions of the normative framework among players (who include current and potential combatants, opinion-makers, lawmakers, decision-makers, and the general public).

Messages conveyed by video games and humanitarian challenges

In this debate it is necessary, first of all, to have a closer look at the messages video games convey. By doing so, their potential undermining effect on perceptions of, and respect for, the fundamental rules of IHL – especially those governing the use of force and the obligation to spare civilians and combatants *hors de combat* – can be better understood. This section highlights several messages video games convey, as well as positive efforts by the video game industry to address the perception issue.

Several messages conveyed by video games are of particular concern precisely because they reflect and reinforce certain ideas that pose a direct challenge

70 For example, in various scenes in the *Call of Duty* games, torture of captives attracts no penalty, whereas in other games shooting civilians results in 'game over'.
71 For example, *Call of Duty* games set in Paris and Tehran.

to IHL. Important examples include the following: war is a law-free zone; the ends justify the means; the means and methods of warfare are not limited; anything living on a battlefield is to be shot at without distinction; identity discs are trophies; and medical staff and facilities can be attacked.

War is a law-free zone

In many video games, inflicting injury or death is normal and the only option available. Impunity is the norm and the law applicable to the situation portrayed in the game is rarely, if ever, acknowledged or enforced. One result is the absence of humanity in video games. In contemporary armed conflicts, the challenge of upholding humanitarian values is not the result of a lack of rules, but a lack of respect for them. Achieving greater respect, implementation, and enforcement of IHL remains an abiding challenge for the international community and a constant priority of the ICRC. This is the responsibility of parties to a conflict, state or non-state, but also requires action by states in peacetime. In addition, sanctions of a disciplinary or criminal nature must be adopted.[72]

The ends justify the means

Some video games require players to witness or participate in graphic scenes of torture and/or murder of enemy captives in order to proceed in the game.[73] In real life, such conduct is absolutely prohibited at all times under both IHRL[74] and IHL.[75] In many video games, enemy fighters are depicted as treacherous villains who broke the rules first. They are often labelled 'terrorists' who deserve brutal treatment including summary execution or torture. A recent challenge for IHL has been the tendency of states to label as terrorist[76] all acts of warfare against them committed by armed groups, especially in non-international armed conflicts. This

72 ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 30th International Conference of the Red Cross and Red Crescent, October 2007, ICRC, pp. 30–31, available at: http://www.icrc.org/eng/assets/files/2011/30ic-8-4-ihl-challenges-report-annexes-eng-final.pdf (last visited 10 January 2012).

73 In *Call of Duty: Black Ops*, players watch a superior coldly execute prisoners of war. Forced onto their knees and begging the executioner for mercy, all prisoners receive a shot to the head, except the last one – who is slain with a knife. On another instance in *Call of Duty: Black Ops*, the player must take part in an act of torture (they must give command for the hero to hit in the face a detainee in whose mouth shards of glass was previously introduced).

74 ICCPR, Art. 7; Convention for the Protection of Human Rights and Fundamental Freedoms, Art. 3; CAT, Art. 2.

75 Common Article 3 of the four Geneva Conventions of 1949 prohibits torture or cruel, inhuman, degrading, or humiliating treatment. See also, Articles 50, 51, 130 and 147 of the four Geneva Conventions respectively, Art. 75 of AP I, Art. 4 of AP II, and CIHL Study, rule 90.

76 There is no commonly agreed legal definition of 'terrorism'. See Additional Protocol II (APII), Art. 4(2)(d). In addition, both Additional Protocols to the Geneva Conventions prohibit acts aimed at spreading terror among the civilian population. See API, Art. 51(2), and AP II, Art. 13 (2). For a discussion on IHL and terrorism, see ICRC, 'International humanitarian law and terrorism: questions and answers', 2011, available at: http://www.icrc.org/eng/resources/documents/faq/terrorism-faq-050504.htm (last visited 10 January 2012).

has created confusion in differentiating between lawful acts of war, including such acts committed by domestic insurgents against military targets, and acts of terrorism.[77]

The means and methods of warfare are not limited

Amongst the weaponry available to players in many video games are explosive devices that are detonated by the presence or proximity of the enemy or on physical contact. On a battlefield and in legal terms such devices would be considered as anti-personnel landmines.[78] Nowadays, some 160 countries have committed themselves to ban these weapons from their military ordinance. Since the Ottawa Convention's adoption fifteen years ago substantial progress has been made in response to the humanitarian issue posed by these mines that keep on killing and maiming long after wars have ended. Nevertheless, great challenges remain, especially in removing remaining mines and relieving the suffering of the hundreds of thousands of injured and their families. In 2009, during the Second Review Conference for the Ottawa Convention, states adopted a plan of action that contains strong commitments to improve work in the fields of victim assistance, stockpile destruction, and mine clearance.[79]

Anything living on a battlefield is to be shot at without distinction

In many first person shooter games, use of force resembles sport. Instead of hunting wild game, players hunt virtual human beings. Since most virtual battlefields are void of civilians, anything living is an enemy.[80] When they are wounded, enemy combatants usually continue fighting thereby justifying their killing. IHL essentially distinguishes between two categories of people in armed conflict: combatants and civilians. While the latter are protected at all times, except and only for such time as they take a direct part in hostilities, the former are protected once out of combat due to illness, injury, capture, or surrender. In contemporary armed conflicts there is a blurring of civilian and military functions. Added to the difficulty of distinguishing

77 See ICRC, above note 72, pp. 6–7. IHL essentially distinguishes between two categories of people in armed conflict, members of the armed forces and civilians. While the latter are protected at all times, except and only for such time as they take direct participation in hostilities, the former are only protected against attack once out of combat (due to illness, injury, surrender, or capture). In contemporary armed conflicts there is a blurring of civilian and military functions. One example is the involvement of civilian agencies (e.g., the CIA drone programme) in military operations. This highlights another difficulty when it comes to distinguishing between civilians and the military: the problem of civilians who directly participate in hostilities.

78 Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction, 18 September 1997, Art. 2.

79 On anti-personnel landmines see, for instance, the ICRC website, available at: http://www.icrc.org/eng/war-and-law/weapons/anti-personnel-landmines/index.jsp (last visited 25 May 2012).

80 One exception is a playable scene from *Call of Duty: Modern Warfare II* that includes the mass killing of civilians inside an airport (although this scene does not take place on a battlefield proper). Players can participate in this killing spree without penalty.

between civilians and the military is the problem of civilians who directly participate in hostilities.[81]

Identity discs are trophies

In recent video games,[82] players must retrieve dog tags from the enemy combatants they have killed in order to validate these kills and be rewarded. In war, many people go missing, causing anguish and uncertainty for their families and friends because their bodies may not be identified. IHL and IHRL require parties to an armed conflict to take measures to ensure that people do not go missing. For instance, all combatants should carry proper identity documents[83] so that their fate can be recorded. The collection of one of the identity discs is authorized under IHL for its transmission to the National Information Bureau or the Central Tracing Agency. The other half should remain with the body to facilitate its identification. In 2003 the ICRC organized an international conference to tackle this hidden tragedy and seek ways to help the families and communities affected. In 2006 the UN General Assembly adopted the International Convention for the Protection of All Persons from Enforced Disappearances.

Medical staff and facilities can be attacked

Another message sent by some video games is that directly targeting medical staff and facilities is normal and triggers no consequences (Figure 3).[84] The impression is reinforced when medics in video games are given offensive roles and weaponry, including grenade launchers.[85] In real armed conflicts thousands of wounded and

81 For the notion of 'direct participation in hostilities' see also, Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, ICRC, Geneva, 2009.

82 These include, in particular, *Call of Duty: Modern Warfare 3* and *Call of Duty: Black Ops 2*.

83 The identity card is the basic document with which the status and identity of persons who have fallen into the hands of the adverse party can be determined, and it must be issued by states to any person liable to become a prisoner of war (GC III, Art. 17). It must contain at least the owner's surname, first names, date of birth, serial number or equivalent information, rank, blood group, and Rhesus factor. As further optional information, the identity card may also bear the description, nationality, religion, fingerprints or photo of the holder, or the date of expiry. In parallel with this measure, the authorities are required to issue specific identity cards for military personnel carrying out special tasks or for certain categories of civilians, The authorities may supplement the above measures by providing identity discs (GC I, Art. 16; GC II, Art. 19). The identity disc is worn permanently round the neck on a chain or strap. It can be a single or double disc made, as far as possible, of durable, stainless material that is resistant to battlefield conditions. The inscriptions it bears are similar to those on the identity card and should be indelible and fade-proof.

84 The Red Cross emblem became synonymous with 'health care' in video games upon the release of *Doom* in 1993. In *ARMA II*, the Red Cross, Crescent, and Crystal emblems are highly visible (Figure 5). Armoured vehicles rigged with an emblem do not carry weapons, only medical equipment. However, 'artificial intelligence' units controlled by the game do not differentiate between persons and objects bearing the protective emblem and those that do not. In the game *Crisis 2*, players can attack an ambulance with impunity. No warnings or penalties are triggered by attacks on ambulances.

85 In multiplayer games each player chooses a class or function. In addition to snipers, grenadiers, or engineers there are often nurses or combat medics whose function is to heal or resurrect fallen comrades. Nurses, sometimes dressed in white and often bearing a Red (or other coloured) Cross, are generally equipped with light weapons and a short reach, but good offensive skills when performing combat

Figure 3. In the game *Crysis 2*, players can attack an ambulance with impunity. No warnings or penalties are triggered by attacks on ambulances. © ICRC, Thierry Gassmann.

sick people are denied effective health care when: hospitals are damaged by explosive weapons or forcibly entered by fighters; ambulances are hijacked; and health-care personnel are threatened, kidnapped, injured, or killed. The problem is so acute in the wars of today that the ICRC is running a global Health Care in Danger campaign to raise awareness about this humanitarian issue.[86]

Innovations by the video games industry addressing humanitarian challenges

Over the last years a number of initiatives have been taken by game designers to address some of the concerns highlighted above. This demonstrates a willingness to 'do the right thing'.[87] Innovations include: the removal of civilians from video games, the introduction of rules and penalties, the reinforcement of the principle of

functions. Such games send several inaccurate messages about the rules of war (e.g., protective emblems may be worn by persons with offensive combat roles, and attacks on medical personnel are acceptable).

86 See ICRC, *Health Care in Danger: A Sixteen-Country Study*, ICRC, Geneva, 2011, available at: http://www.icrc.org/eng/assets/files/reports/4073-002-16-country-study.pdf (last visited 2 August 2012). States and Red Cross and Red Crescent National Societies unanimously passed a resolution on this issue at the 31st International Conference of the Red Cross and Red Crescent. See 'Resolution 5, Health Care in Danger: Respecting and Protecting Health Care', document prepared by the ICRC, adopted at the 31st International Conference of the Red Cross and Red Crescent, Geneva, 28 November–1 December 2011, available at: http://www.rcrcconference.org/docs_upl/en/R5_HCiD_EN.pdf (last visited).

87 See for example changes between *Battlefield 1* and *3*. In the later version, players do not have to see or act out torture.

distinction, the provision of options other than killing, the removal of the Red Cross and Red Crescent emblems, and the inclusion of warnings and target restrictions to the players.

Removal of civilians from video games

After observing that players shoot innocent civilians in video games 'simply because they can', the creators of *Battlefield 3* decided to remove all civilians from their game and sideline the issue of distinction.[88] However, this rather radical solution leads to some unrealistic depictions of urban conflict, including fighting taking place in city centres devoid of civilians.[89]

Introduction of rules and penalties

In an attempt to mirror battlefield reality some video game designers have built rules and penalties into the script. In doing so they have integrated aspects of the law applicable during a real armed conflict. In some games, characters are penalized for killing civilians. For example, in *Dar al-Fikr – Under Ash*, produced by the Syrian creators of *Under Siege*, shooting civilians triggers a loss of points or 'game over'. In *Rainbow Six: Vegas*, 'excessive' killing of civilians is punished by removing the player from command.[90] In *ARMA II*, players can shoot unarmed civilians. However, if they persist with such behaviour they will eventually be shot by soldiers from their own side.[91]

Reinforcement of the distinction principle

In *Call of Duty – Modern Warfare 3*, the majority of enemy soldiers are depicted wearing distinct uniforms and emblems, and act largely within the bounds of IHL. In those parts of the story where they are not in uniform, enemy fighters are distinctly armed and intent on harming the player, causing no confusion about who is and who is not a legitimate target.[92]

88 Alec Meer, 'Why you can't shoot civilians in *Battlefield 3*', interview of Patrick Bach CEO of DICE, *in Rock, Paper Shotgun*, 30 August 2011, available at: http://www.rockpapershotgun.com/2011/08/30/why-you-cant-shoot-civilians-in-battlefield-3/ (last visited 2 August 2012).

89 While civilians may not be visible in the game, it is difficult to imagine an armed conflict taking place in downtown Tehran (*Battlefield 3*) or Paris (*Call of Duty: Modern Warfare 3* and *Battlefield 3*) without any civilians being present.

90 F. Castillo, above note 51, p. 37.

91 Alternatives to the use of lethal force against friendly forces include allowing players to arrest and court-marshal soldiers that commit war crimes. The challenge for designers is to find ways to implement such changes without affecting the flow of the game.

92 Unlike early versions of these games, *Call of Duty 4* and *Halo 3* also integrate changes to avoid improper use of the emblems. For example, the Red Cross emblem is no longer used in these games as an indicator of how players can recuperate and replenish their health.

Provision of options other than killing

While IHL permits the use of lethal force against enemy combatants and military objectives,[93] the parties to an armed conflict are free to achieve their military aims without resorting to the use of lethal force. In a bid to better reflect reality, some games include options, other than killing the enemy, to achieve certain objectives. In Hezbollah's video game, *Special Force 2*, the objectives include capturing enemy soldiers. *ARMA II* is the only game, known to the authors, that includes a 'surrender option' for players or enemy troops.[94] In *Under Siege* the hero rescues wounded Palestinians shot by the enemy.

Removal of the Red Cross and Red Crescent emblems

In some video games the Red Cross and Red Crescent protective emblems are replaced with alternatives (usually blue, green, or white crosses).[95] Nevertheless, replacing the protective emblems with other symbols does not change the fact that medical personnel and volunteers who engage in medical tasks must always be respected and protected, unless they commit, outside of their humanitarian function, acts harmful to the enemy.[96]

Warnings and target restrictions

Another innovation in game design is the inclusion of warnings for players against acts that could be construed as violations of IHL if they occurred in a real armed conflict. In *Call of Duty – Modern Warfare 3*, game makers have gone to some lengths in Version 3 to avoid making civilians and civilian infrastructure targets (a feature of Version 1).[97] Where civilian objects become military targets, the game explains why. When civilians are in the player's line of fire, an invisible commander announces that they are civilians and instructs the player to either hold fire or aim with care. If the player chooses to shoot a civilian, the mission instantly ends in failure and the game explains why.[98]

93 Subject always to the rules on distinction, proportionality, and precautions.

94 In direct contrast to IHL, the general rule in video games is that 'no one surrenders' to enemy fighters. The requirement to release the enemy if they cannot be detained is entirely absent. As noted above, in games tested by the ICRC, wounded persons generally struggle or try to fight back with a firearm. Others just wait until their adversary kills them. In some (unplayable) scenes, injured fighters are shot at while trying to surrender.

95 An exception is *ARMA II*, which includes three of the distinctive emblems of the Red Cross and Red Crescent Movement.

96 When they carry and use light weapons to defend themselves or to protect the wounded and sick in their charge, medical personnel do not lose the protection to which they are entitled. The wounded and sick under their care remain protected even if the medical personnel themselves lose their protection. See AP I, Art. 13, rules 25 and 28 of the ICRC Customary Law Study (see also p. 85 of the commentary to rule 25, in the ICRC Customary Law Study, above note 52).

97 For several problematic scenes in Version 1 of *Call of Duty – Modern Warfare 3*, see F. Castillo, above note 51, pp. 23–25.

98 Such innovations suggest the involvement of military and/or legal advisors in game design. See also, Dave Their, 'The real soldier behind the 'Call of Duty' games', in *The Washington Post*, 19 October 2010,

Figure 4. Summary execution of a captive in *Call of Duty: Modern Warfare II*. Players must view this unplayable scene to proceed further in the game. No penalties, warnings, or consequences accompany this scene. © ICRC, Thierry Gassmann.

ICRC initiative

On the basis of field experience and research[99] the ICRC has come to the conclusion that behaviour is more effectively changed by modifying the environmental conditions that influence it than by directly trying to alter people's opinions, attitudes, or outlook. Accordingly, the ICRC's activities aim to prevent human suffering caused by armed conflict and other situations of violence by fostering an environment conducive to respect for the life and dignity of persons affected by armed conflict and other situations of violence, and respect for humanitarian work. With respect to video games and individual behaviour, there is no conclusive scientific basis for linking IHL violations that occur in real life with those depicted in video games. Nonetheless, it is contended that the widespread use of video games has the potential to desensitize players to the very existence of rules on the use of force.

Considering the potential of video games to convey both positive and negative messages to players regarding what is a permissible conduct during armed conflict, the ICRC is concerned that a range of video games are trivializing heinous behaviour such as torture and summary execution (Figure 4). New releases continue

available at: http://www.aolnews.com/2010/10/19/the-real-soldier-behind-the-call-of-duty-games/ (last visited 30 July 2012).

99 D. Muñoz-Rojas and J.-J. Frésard, above note 33.

Figure 5. The Red Cross, Red Crescent, and Red Crystal emblems are rarely displayed in today's video games. An exception is *ARMA II*. In this screen shot, a medic treats a wounded fighter next to medical post and vehicle marked respectively with the Red Cross and Red Crystal emblems. © Bohemia Interactive.

to allow players to perform, without penalty, acts that would constitute violations of IHL if they occurred in a real armed conflict. In 2011 the ICRC invited states and Red Cross and Red Crescent National Societies to a presentation on video games that portray contemporary armed conflicts. A short film, highlighting scenes from some of the world's most popular video games, including the *Medal of Honor, Call of Duty*, and *ARMA* franchises, generated a vibrant discussion, both at the event and subsequently online, about whether rules of IHL should be integrated into video games. In raising these concerns, the ICRC has emphasized that it does not propose a ban on the depiction of violence in video games. Nor is it calling for further regulation of the video game industry. As paradoxical as it may appear, the ICRC does not advocate for video games in which violations are prohibited. Violations occur on real battlefields and may therefore also take place in video games. However, the ICRC does call for the depiction of battlefields that mirror reality. Some recent releases, including *ARMA II* (see Figure 5), represent an important shift in this direction. This requires the portrayal of military operations regulated by law and the presence of civilians and civilian objects so that the principles of distinction and proportionality can be properly understood and respected. Players who act out combat roles should face the same dilemmas and challenges as real combatants do. Characters who break the rules in video games should be subject to penalties and punishments as real combatants.

Considering the positive steps already taken by some designers to integrate aspects of the rules governing the use of force, the ICRC, together with a number of Red Cross National Societies, seeks to work with the industry in order to influence

major video games. The overall objective is to see a change of behaviour on the part of the industry leading to the inclusion, in new video games or new versions of existing ones, of penalties for violations of the rules of war, when such violations are possible within the parameters of the game.

Since its creation in 1863, the ICRC has gained extensive first-hand experience of armed conflicts and other situations of armed violence. Thanks to its work with government authorities, non-state armed groups, the military, police, and others for the adoption of preventive measures for the respect of the law, the ICRC may offer useful advice to the industry in their endeavours. Together with concerned Red Cross and Red Crescent National Societies it has initiated a dialogue with game producers, designers, and players on the production of more realistic games that integrate the law and therefore present players with the same dilemmas as those faced by soldiers on contemporary battlefields. The outcome of this initiative will be measured by the content of video games released by December 2013.

The aim is not to spoil players' enjoyment by, for example, interrupting game play with pop-up text listing legal provisions or lecturing gamers on the rules of war. Instead, the aim is to see rules governing the use of force integrated into video games so players can have a truly realistic experience and deal first hand with the principles of distinction (by verifying the nature of targets), proportionality (by choosing the course of action that will cause the least incidental damage to civilians and their property), and precautions (by deciding whether attacks can proceed or must be delayed or aborted). Consequently, persons and objects protected by IHL need to be included if the game is to reflect the realities of armed conflicts.

By way of example, a more realistic approach to the issue of the respect of medical units and to the use of protective emblems would be to retain the Red Cross and Red Crescent emblems in video games, highlight their protective and indicative functions,[100] and introduce penalties when players attack medics, medical transports, and hospitals displaying the emblem. Penalties should also apply if a player misuses or abuses the emblem (for example, by transporting weapons to the frontline in ambulances or launching attacks from ambulances (the war crime of perfidy)).[101]

Initiatives already taken by the industry demonstrate the feasibility of such solutions. In a survey of gamers most respondents supported the idea that a player

100 See ICRC, *Study on the Use of the Emblems: Operational and Commercial and other Non-operational Issues Involving the Use of the Emblems*, ICRC, Geneva, 2011.

101 Art. 37 of AP I prohibits acts of perfidy or 'inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence'. Examples include: feigning intent to surrender or negotiate under a flag of truce; feigning incapacitation by wounds or sickness; feigning civilian, non-combatant status; and feigning protected status by the use of signs, emblems, or uniforms of the UN or of neutral or other states not Parties to the conflict'. The Rome Statute of the International Criminal Court (hereinafter Rome Statute), opened for signature 17 July 1998, 2187 UNTS 3 (entered into force 1 July 2002), includes as war crimes, the improper use of distinctive emblems resulting in death, serious injury, intentional attacks on buildings, material, medical units and transport and personnel using the distinctive emblems of the Geneva Conventions. See Art. 8(2) (b)(vii) and (xxiv), and (e)(ii) of the Rome Statute.

who respects the rules of war in a video game should be rewarded for doing so.[102] Conversely, those who break the rules should be sanctioned. Strong sales of new releases that have integrated rules of war provide evidence that integrating the law does not undermine the commercial success of video games.[103]

Conclusion

This article has called for more realistic video games where players face the same dilemmas as combatants. Considering the mechanisms at play in video games and their pedagogical value, it is argued that players should be rewarded when they respect the law and sanctioned if they violate it. Undoubtedly, video games represent an important vector through which applicable rules on the use of force and the treatment of persons in the hands of the enemy can be identified or ignored. In the view of the authors, their reach far exceeds that of traditional IHL and IHRL education and training programmes.[104] Those who have doubts about the importance of video games for the dissemination of humanitarian norms need look no further than the size of the video game industry; the limited awareness of IHL and IHRL among players of video games[105] and the general public;[106] the large number of military personnel recruited through video games; and the higher than average rate of video game play by serving military personnel.[107] A number of questions pertaining to video games require further research. The potential for drone pilots to bring a 'PlayStation mentality' to work and the possible impact on decision-making during military operations is an important example. Another is the nature and scope of IHL and IHRL obligation of states with respect to commercial video games. It is the authors' hope that this article may serve as a source of inspiration for others to examine, in greater depth, these and other questions concerning the relation between video games and humanitarian norms.

102 G. Humbert-Droz, above note 15. According to this French language survey, few players knew much about IHL. Interest in integration of IHL into video games was low.

103 For instance, in 2012, *Call of Duty: Modern Warfare 3* (in which game-makers have gone to some lengths to avoid making civilians and civilian infrastructure targets – a feature of Version 1) ranked number eight within the top ten best-selling games and number two among first person shooter games depicting combat situations (*Call of Duty; Black Ops 2* being number one). See '10 best selling videogames in 2012', above note 4.

104 According to McGonigal, tens if not hundreds of millions of people play video games each year. See Jane McGonigal, 'Gaming can make a better world', TED Talk filmed in February 2010, available at: http://www.ted.com/talks/jane_mcgonigal_gaming_can_make_a_better_world.html (last visited 30 July 2012). See also Entertainment Software Association, *Sales, Demographic and Usage Data: Essential Facts about the Computer and Video Game Industry*, Entertainment Software Association, Washington, D.C., 2011, available at: http://www.theesa.com/facts/pdfs/ESA_EF_2011.pdf (last visited 30 July 2012).

105 See G. Humbert-Droz, above notes 15 and 102.

106 See B. A. Gutierrez, S. DeCristofaro and M. Woods, above note 18, p. 1038 ('many Americans have never been taught about the Geneva Conventions, except perhaps that they exist . . . two in five young people and one in three adults in the US believe that American soldiers detained abroad can be tortured').

107 See B. W. Knerr, above note 21.

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

Documenting violations of international humanitarian law from space: a critical review of geospatial analysis of satellite imagery during armed conflicts in Gaza (2009), Georgia (2008), and Sri Lanka (2009)

Joshua Lyons

Josh Lyons is the satellite imagery analyst at Human Rights Watch (HRW). Before joining HRW, he was the principal analyst of the UN's operational satellite applications programme (UNOSAT). Mr Lyons has master's degrees in international relations from the London School of Economics (LSE), and geographic information science from University College London (UCL).

Abstract

Since the launch of the first commercial very high resolution satellite sensor in 1999 there has been a growing awareness and application of space technology for the remote identification of potential violations of human rights and international humanitarian law. As examined in the three cases of armed conflict in Gaza, Georgia,

doi:10.1017/S1816383112000756

and Sri Lanka, analysis of satellite imagery was able to provide investigators with independent, verifiable, and compelling evidence of serious violations of international humanitarian law. Also examined are the important limitations to such imagery-based analysis, including the larger technical, analytical, and political challenges facing the humanitarian and human rights community for conducting satellite-based analysis in the future.

Keywords: satellite imagery, armed conflict, international humanitarian law, IHL, Gaza, Georgia, Sri Lanka, space technology, human rights, geospatial, GEOINT, human rights Watch, HRW, Richard Goldstone, UNOSAT, South Ossetia, damage assessment, Tamil Tigers, LTTE, Goldstone Report, Israel, IDF, United Nations, UN, UNITAR, IMINT.

The application of satellite technology for the remote identification of potential violations of international humanitarian law (IHL) was clearly demonstrated by the selective release of US intelligence imagery over suspected mass graves in Srebrenica in 1995 and Kosovo in 1999.[1] The first open source demonstration came with the commercial release of Ikonos satellite imagery over the city of Grozny in March 2000, a month after the Russian army occupied the city during the Second Chechen War.[2] As shown in Figures 1 and 2, the near total destruction of several thousand buildings within central Grozny was irrefutably documented in graphic detail. The implications were as dramatic as they were obvious: commercial satellite imagery had now made it possible for international investigators to collect evidence on alleged war crimes remotely from the conflict zone, during active hostilities, and independent of the traditional need to secure official permission from one or more parties to the conflict.

Since the release of the first commercially available very high resolution (VHR) satellite imagery in late 1999[3] there has been a growing awareness of the potential of this space technology for the independent monitoring and analysis of events on the ground during periods of armed conflict, and specifically as a source of evidence for serious violations of IHL.

1 Yahya A. Dehqanzada and Ann M. Florini, 'Secrets for sale – how commercial satellite imagery will change the world', Carnegie Endowment for International Peace, February 2000, available at: http://carnegieendowment.org/2000/03/01/secrets-for-sale-how-commercial-satellite-imagery-will-change-world/4jgy (last visited 25 March 2012). See also Lt Col. Peter L. Hays, 'Transparency, stability, and deception: military implications of commercial high-resolution imaging satellites in theory and practice', presented at the International Studies Association Annual Convention, Chicago, 21–24 February 2001, available at: http://isanet.ccit.arizona.edu/archive/hays.html (last visited 25 March 2012).

2 Imagery courtesy of GeoEye 2012. The UN characterized Grozny in 2003 as 'the most destroyed city on earth'. See 'Scars remain amid Chechen revival', in *BBC News*, 3 March 2007, available at: http://news.bbc.co.uk/2/hi/programmes/from_our_own_correspondent/6414603.stm (last visited 25 March 2012).

3 The Ikonos satellite based on declassified US military technology. VHR imagery is generally defined by a spatial resolution (the minimum image pixel size) of one metre or less in diameter, a threshold that enables the visual identification of many terrestrial objects, including small passenger vehicles, makeshift refugee shelters, and building damages.

Figure 1: Central Grozny (Minutka Sq.) on 16 December 1999 (Image © GeoEye).

Over the last thirteen years the number of commercial and dual-use[4] satellite sensors has rapidly grown to over ten, providing a remote monitoring and analytical capacity which has been successfully employed in a modest but growing number of cases, covering the full conflict spectrum from traditional inter-state and civil wars, to cases of counterinsurgency and organized intercommunal violence.

Detailed analysis of commercially available satellite imagery can, under specific circumstances, have an important planning and verification role within the investigative process. It can provide valuable insights into the spatial and temporal context of the conflict, it can help identify specific areas or incidents for further review, and it can help confirm or challenge testimony of uncertain reliability.

Most importantly, satellite analysis can provide independent, verifiable, and compelling evidence of serious violations of IHL covering, for example, the use of indiscriminate and disproportionate force in civilian areas; the targeting of protected humanitarian and cultural sites; the use of civilians as human shields; the destruction of installations containing dangerous forces; and the failure to exercise precautionary measures to protect civilians from the effects of attacks.[5]

However, for all the compelling cases where satellite imagery has played a significant and dynamic role in monitoring armed conflicts and documenting

4 Dual-use satellite systems are jointly developed, financed, and controlled through bilateral agreements between private companies and national intelligence agencies or military agencies.

5 Covered in Articles 51, 53, 56, and 57 of Additional Protocol I of the Geneva Conventions of 12 August 1949, Articles 11, 15 and 16 of Additional Protocol II, and relevant customary IHL rules.

Figure 2: After Russian occupation on 16 March 2000 (Image © GeoEye).

potential war crimes, there are also multiple cases where it provided inconclusive, ambiguous, and sometimes misleading or erroneous results which have generally gone underreported, creating a distorted perception of the overall efficacy of space technology, and consequently raising unrealistic expectations within the international humanitarian community.

One important objective of this emerging field of applied humanitarian research should be a more self-critical understanding of the inherent limits to imagery analysis, as well as the potential political and legal consequences of conducting incomplete, erroneous, or otherwise misleading analytical work over conflict zones. Considering the increasing interest in and potential adoption of such technical capacity within humanitarian agencies and non-governmental organisations (NGOs) there is a corresponding need for more rigorous debate and the open exchange of lessons learned and best practices.

Primary applications of satellite analysis for international humanitarian law

Based on the practical experience of United Nations (UN) agencies and international and non-governmental organisations in the 2000s, satellite-based monitoring and analysis applications fall into two application levels. The first is

providing direct support to traditional field-based investigations of alleged war crimes. The second is substituting for these field-based investigations. The distinction between these two application levels has generally depended on the quantity and relevance of the available satellite data and, most importantly, on the overall level of political and physical access to the affected areas and people under investigation.

Imagery analysis in support of field-based investigations

When direct and meaningful field access is possible, satellite analysis can provide a range of analytical and technical support to traditional investigations by improving the overall planning, quality, and accuracy of field-based work. Specifically, satellite analysis can have an investigative multiplier effect by, for example, identifying and evaluating sites of interest before mission deployment, thereby potentially saving significant time and resources. It is often the case that detailed imagery coverage and analysis can provide a more accurate estimate of the total number of people or the infrastructure affected when alleged violations took place months or even years earlier leaving little remaining physical evidence, or the estimate is based on the testimony of survivors from a small and potentially non-representative sample of affected communities.

Investigators have more frequently relied on satellite data and analysis to provide corroborative evidence to help evaluate the accuracy of reported incidents or claims from sources of unknown reliability. When there is sufficient spatial and temporal coverage of satellite imagery that can be accepted and referenced as an objective baseline dataset, it can provide a common operational picture of the situation on the ground thereby helping to clarify events when multiple, contradictory reports or testimonies present a disputed or uncertain understanding of relevant events and locations.

Because of the near-real time capacity of satellite sensors to provide detailed imagery normally within twelve to twenty-four hours, it has become a de facto standard used to rapidly evaluate reported events that have not yet been independently verified in the field. An interesting dynamic in this context is the observed tendency for agencies and organisations responsible for imagery analysis to publicize only 'successful' cases of positive confirmation of expected outcomes or reported events. Although there has been no systematic effort to document the number of false-positive claims successfully challenged by the rapid assessment of satellite imagery, it is almost certainly the case that the number is significantly underestimated. This probable tendency to underreport findings that run counter to expected or feared claims of potential war crimes is understandable considering the emotive context, but nevertheless tends to undervalue the full range of potential benefit that imagery can provide for investigations.

During the Georgian conflict (2008), for example, a UN agency requested rapid imagery collection to assess claims made by the Georgian foreign ministry that 'the Black Sea port of Poti, the site of a major oil shipment facility, had been

"devastated" by a Russian air raid'.[6] Surprisingly, the imagery collected revealed little evidence of aerial bombardment, let alone of devastating damages to the port facility or adjacent civilian residential buildings. Instead, the imagery assessment identified six Georgian navy vessels that had been scuttled in the harbour, presumably by elite Russian forces who had reportedly occupied the port facilities for several hours.[7]

In another instance during the same Georgian conflict, reports of widespread and deliberate destruction of cultural heritage sites in the Tskhinvali region led Georgian officials to urgently request a detailed satellite assessment by the UN. The findings showed that although at least three religious monuments had likely been destroyed, the majority of sites of concern showed no indications of damage. It was eventually concluded, much to the relief of Georgian officials, that there was little evidence to suggest a deliberate campaign by South Ossetian militias of systematic destruction of Georgian historic monuments in the area, as originally feared.[8]

Imagery analysis as a primary source

The second and perhaps more significant application area for satellite-based analysis is as a primary source of direct evidence relating to potential serious violations of IHL. Imagery analysis can be used when on-site investigations and access to witnesses are impossible normally due to insecurity, government prohibitions, or physical inaccessibility. Under these circumstances, satellite imagery has proved to be one of the only viable means of independent, objective, and systematic collection of significant evidence of possible war crimes, as originally demonstrated over the city of Grozny during the second Chechen war in 2000. As will be examined in the cases of Georgia (2008) and Sri Lanka (2009), it was precisely the combination of relevant imagery coverage and a sustained lack of physical access to the conflict zones that made the analysis of satellite data critical to the overall understanding and investigation of the conflicts.

Three case examples: Gaza (2009), Georgia (2008), and Sri Lanka (2009)

These three cases were selected because of the relative importance that satellite imagery analysis played in the context of the conflicts, providing meaningful support as well as direct primary evidence to investigations of alleged violations of IHL.

6 'Russian jets attack Georgian town', in *BBC News*, 9 August 2008, available at: http://news.bbc.co.uk/2/hi/europe/7550804.stm (last visited 15 April 2012).

7 Satellite imagery assessment done by UNITAR – operational satellite applications programme (UNOSAT). Overview map available at: www.unitar.org/unosat/node/44/1262 (last visited 25 April 2012).

8 Based on author's unpublished correspondence and notes. See 'Satellite damage assessment for cultural heritage monuments, South Ossetia, Georgia', UNITAR, available at: http://www.unitar.org/unosat/node/44/1265 (last visited 25 April 2012).

Although these specific cases are in many respects strong illustrations of the larger significance and long-term potential of satellite technology for such work, critical limitations and challenges that were identified at the time will be examined as well.

Gaza (2009)

Immediately after the start of the Israeli military operation Cast Lead in late December 2008, satellite-based monitoring and damage assessments over Gaza were initiated by the UN's operational satellite applications programme (United Nations Institute for Training and Research/UN operational satellite applications programme (UNITAR/UNOSAT)) to support ongoing emergency humanitarian operations on the ground. A detailed series of damage-assessment-focused products were publicly released[9] and the satellite-derived datasets shared with humanitarian organisations, such as the International Committee of the Red Cross, and human rights organisations, such as Human Rights Watch, for their own internal work.

Within days of the Israeli withdrawal from Gaza, satellite-based analysis by the UN had compiled a list of over 3,800 individual damage sites within the Gaza Strip, including almost 2,700 damaged buildings, 187 demolished greenhouse complexes, and 930 impact craters on main roads and open/cultivated fields.[10] Based on the specific damage signatures, the detection of Israeli Defence Forces (IDF) ground forces and associated vehicle patterns, it was generally possible to attribute the damage to Israeli Air Force (IAF) air strikes, IDF heavy artillery fire, or demolition by IDF tank and bulldozers.[11]

Following the establishment of the UN Fact Finding Mission on the Gaza Conflict by the UN Human Rights Council in April 2009,[12] the appointed head of the Mission, Judge Richard Goldstone, commissioned additional satellite imagery analysis to support the Mission's investigation.[13] Maps and associated documents provided the Goldstone Mission with a comprehensive overview of the relative magnitude and spatial distribution of damages within Gaza. As Goldstone publicly commented after the completion of the official Report of the United Nations Fact Finding Mission on the Gaza Conflict:[14]

> . . . we commissioned . . . a full satellite report, which is part of our report. It's a thirty-four-page report with satellite photographs of Gaza before and after the

9 See products available at: http://www.unitar.org/unosat/maps/PSE (last visited 25 April 2012).

10 'Satellite-based Gaza damage assessment overview', UNOSAT, available at: http://unosat-maps.web.cern.ch/unosat-maps/PS/Crisis2008/UNOSAT_GazaStrip_Damage_Review_19Feb09_v3_Lowres.pdf (last visited 25 April 2012).

11 *Ibid.*, attribution to the different Israeli military branches was possible to an uneven extent, depending on the relative complexity of the environment and level of damages detected.

12 UN GA Res. 60/251, 3 April 2009.

13 'Satellite image analysis in support to the United Nations Fact Finding Mission on the Gaza Conflict', UNITAR/UNOSAT, 31 July 2009, available at: http://www2.ohchr.org/english/bodies/hrcouncil/special-session/9/docs/UNITAR_UNOSAT_FFMGC_31July2009.pdf (last visited 25 April 2012).

14 Report of the United Nations Fact Finding Mission on the Gaza Conflict, UN Doc. A/HRC/12/48, 25 September 2009, available at: http://www2.ohchr.org/english/bodies/hrcouncil/specialsession/9/factfindingmission.htm (last visited 25 April 2012).

> Israeli Defence Force campaign. And we used that to corroborate or not corroborate a lot of the information we got with regard to damage.[15]

The fact-finding report used a range of quantitative information derived from satellite imagery on the timing of Israeli attacks to corroborate eyewitness testimonies and, more significantly, as primary evidence that was cited as part of the legal findings of grave breaches of the Fourth Geneva Convention by Israeli forces.[16]

The section of the report that focused on incidents of 'deliberate attacks against the civilian population' cited, several times, UNOSAT figures on the number of building damages in residential areas of Gaza and the period in which they occurred. These were used to corroborate testimonies of individual families in relation to high-profile incidents such as the death of twenty-three members of the al-Samouni family in the Zeytoun neighbourhood of Gaza governorate.[17]

The most extensive reliance of the Mission on imagery analysis was in the section of the report on 'destruction of industrial infrastructure, food production, water installations, sewage treatment plants, and housing'.[18] In addition to detailed observations on the apparent Israeli targeting of a number of important industrial facilities, UN imagery analysis provided the only comprehensive information on the scale of destruction of greenhouse complexes throughout the Gaza Strip, destruction that the Mission concluded 'was not justified by any possible military objective'.[19]

Further, in multiple locations throughout the Gaza Strip a spike in Israeli attacks against commercial and residential buildings was observed during the final days of the conflict, immediately preceding the ceasefire and the withdrawal of IDF ground forces. Quantitative figures derived from the imagery documenting this trend raised direct questions about IAF targeting strategy and the issue of operational necessity. In the case of Rafah, for example, a distinct shift in IAF targeting was observed in the last week of the conflict. Between 27 December 2008 and 10 January 2008, IAF air strikes were concentrated in empty fields running along the Philadelphi Corridor of the border in reported attempts to destroy the underground tunnels between Gaza and Egypt. However, during the final week of the conflict leading up to the Israeli-declared ceasefire on 18 January 2009, there were indications that IAF air strikes had shifted from targeting underground tunnels to the destruction of over 500 buildings situated along the border.[20]

Similar patterns of heavy destruction of buildings in the final days of the conflict were identified from satellite imagery from multiple neighbourhoods in the governorates of Gaza and Gaza North, including the al Atatra area that sustained

15 'Goldstone transcript: righteous in our generation', Rabbibrian's Blog, available at: http://rabbibrian.wordpress.com/2009/10/23/goldstone-transcript-righteous-in-our-generation/ (last visited 25 April 2012).
16 UN Fact Finding Mission Report, above note 14, para. 1006.
17 *Ibid*., pp. 160 and 174.
18 *Ibid*., pp. 205–208, and pp. 214–217.
19 *Ibid*., para 1021.
20 Satellite image analysis in support to the United Nations Fact Finding Mission on the Gaza Conflict, UNITAR/UNOSAT, 27 April 2009, pp. 6–13.

destruction of over 55 per cent of its buildings during the last three days of the conflict.[21]

As the Mission report concluded in its legal findings on the timing of building destruction during the final stages of the conflict:

> Combining the results of its own fact-finding on the ground with UNOSAT satellite imagery and the published testimonies of Israeli soldiers, the Mission concludes that, in addition to the extensive destruction of housing for so-called operational necessity during their advance, the Israeli armed forces engaged in another wave of systematic destruction of civilian buildings during the last three days of their presence in Gaza, aware of their imminent withdrawal. The conduct of the Israeli armed forces in this respect violated the principle of distinction between civilian and military objects and amounted to the grave breach of 'extensive destruction … of property not justified by military necessity and carried out unlawfully and wantonly'.[22]

Overall, satellite data analysis clearly served an important investigative function that helped to structure and focus the Mission's work, raise confidence levels in collected testimonies by providing independent corroboration, as well as offer independent, primary evidence cited directly in some of the legal findings of the Mission report.

Although covered in more detail below in this article, it is important to acknowledge that there were significant and sometimes glaring limits to the applicability of satellite imagery analysis in the case of Gaza. Of particular concern was the inability, because of a systematic lack of accurate GPS data on important facilities throughout Gaza, to locate in the satellite imagery several important factories, schools, and hospitals of direct interest to the Mission investigation. More problematic was the failure to produce any relevant information on potential IHL violations committed by Hamas, including deploying their forces in populated areas without taking all feasible steps to minimize harm to civilians, or committing war crimes by deliberately using civilians as human shields – a significant shortcoming with direct implications for the monitoring and analysis of asymmetrical conflicts more broadly. Another limitation was the inability to produce relevant information on the potentially restricted use of certain weapons systems, such as white phosphorus, by IDF forces. These and other limitations of the work during the Gaza conflict will be covered in more detail below in the section 'Satellites to the rescue?'

Georgia (2008)

Following the Georgian military assault on South Ossetian and Russian forces in Tskhinvali on 7–9 August 2008, and the later withdrawal of the Georgian forces from the city on 13 August 2008, the UN initiated a satellite-based monitoring and damage assessment project at the request of several agencies and

21 *Ibid*., pp. 14–22.
22 UN Fact Finding Mission Report, above note 14, paras. 53 and 1006.

organisations.[23] Based on initial reports of heavy Georgian artillery and Grad rocket fire against Ossetian positions, the new imagery was initially focused on the city of Tskhinvali; however, it quickly became apparent that an enlarged assessment beyond Tskhinvali would be needed to cover a second wave of violence apparently taking place to the north and east of the city.

Drawing on lessons learned from the monitoring of post-election arson attacks in Kenya earlier in January 2008,[24] it was possible to use satellite data obtained from environmental sensors to identify and monitor the outbreak of large fires occurring in multiple locations within South Ossetia immediately following the withdrawal of Georgian forces. Although the environmental sensors employed[25] could not distinguish actual building damages or determine the cause of the fires, it was reasonably inferred from the timing and location that the sudden outbreak of fires occurring simultaneously in multiple locations was unlikely to have been caused by accidental or natural causes. A more reasonable explanation was that such fires represented a campaign of arson directed against ethnic Georgian villages – an interpretation confirmed by eyewitness testimony and field photos recorded by Human Rights Watch researchers in South Ossetia at the time of the attacks.[26]

Daily monitoring of active fire locations revealed a pattern of suspected arson starting on 10 August immediately north of Tskhinvali and rapidly expanding in number and extent on 12 August, reaching as far as the ethnic Georgian villages of Kekhvi to the north and Eredvi to the east. As the fires continued on the following days, it was possible to identify from the cumulative distribution of detected fire locations that two distinct clusters of suspected arson attacks were forming, the first centred on ethnic Georgian villages located along the main road (Route P-2) and the Liakhi River north of Tskhinvali, and the second cluster located along a secondary road east of Tskhinvali between the villages of Pirsi and Eredvi (see figure 3).

Analysis of very high resolution satellite data acquired on 19 August 2008 provided further evidence of the arson campaign with the dramatic capture in the imagery of at least eight active building fires. As illustrated in Figure 4, a residential building located in the village of Kurta was clearly on fire with an associated plume of dark smoke. Also visible within the satellite imagery were hundreds of small, residential buildings with distinct arson-related damage signatures, such as the lack of building rooftops but with intact load bearing walls, consistent with the stone wall/wood roof construction typical of the region.

A rapid damage assessment of the affected villages in the region was conducted using the satellite imagery from 19 August. Results of the assessment

23 Project work conducted by UNITAR/UNOSAT 2008.

24 Example of arson overview product available at: http://www.unitar.org/unosat/node/44/1035 (last visited 29 April 2012).

25 Fire data obtained from two NASA satellites MODIS Aqua and Terra, which together provided data on probable active fires within an approximate area of one square kilometre upwards of two to four times daily.

26 Based on internal UN correspondence. See also 'Georgia: satellite images show destruction, ethnic attacks', in *Human Rights Watch*, 28 August 2008, available at: http://www.hrw.org/news/2008/08/27/georgia-satellite-images-show-destruction-ethnic-attacks (last visited 25 April 2012).

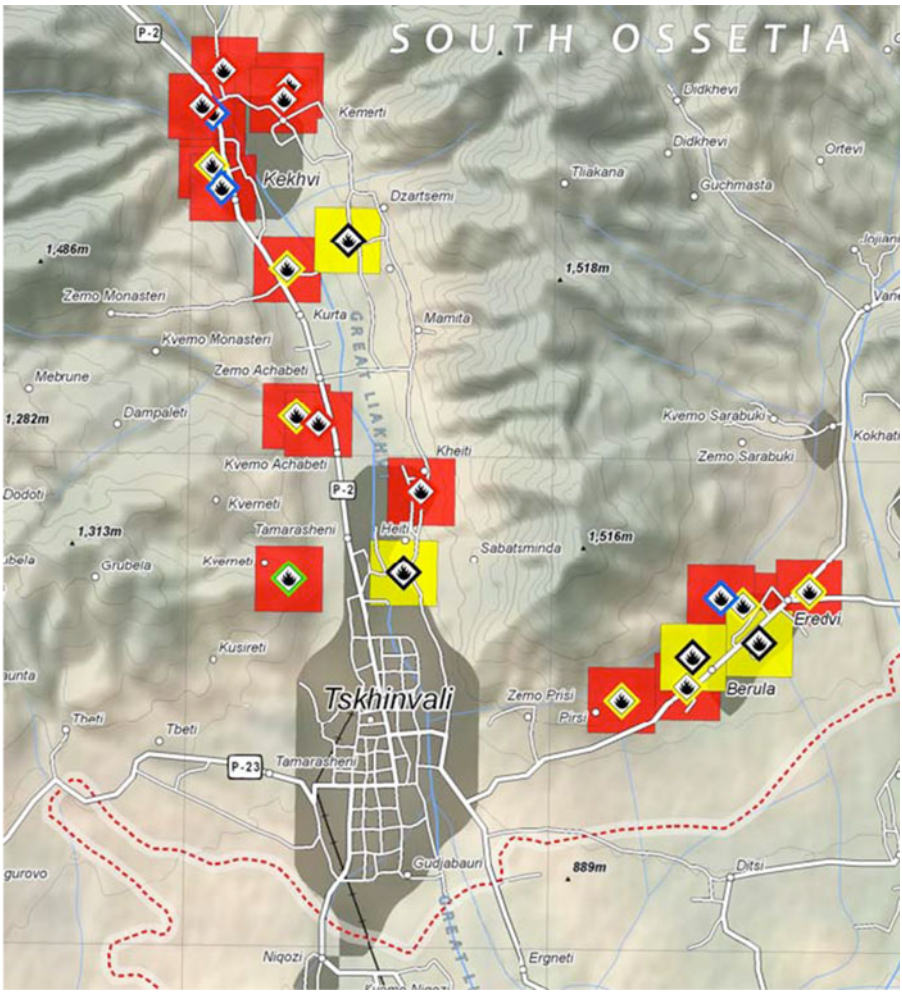


Figure 3: Map of suspected arson attacks in South Ossetia (Image © UNITAR/UNOSAT).

were publicly released in the form of maps, with figures on the number of destroyed and severely damaged buildings aggregated by affected village. For the initial results covering the first cluster of building damages, including the city of Tskhinvali northward to the village of Kekhvi, a total of 1,050 buildings were either destroyed or severely damaged. For the second damage cluster located east of Tskhinvali between the villages of Pirsi and Eredvi, a further 300 buildings were either destroyed or severely damaged.[27]

27 'Village damage summary: Kekhvi to Tskhinvali, South Ossetia, Georgia', UNITAR, 28 August 2008, available at: http://www.unitar.org/unosat/node/44/1258 (last visited 29 April 2012). Figures for building damages were all based on final post-conflict images recorded on 19 August 2008. Based on the fact that

Figure 4: Residential building on fire after arson attacks in village of Kurta, South Ossetia (Image © DigitalGlobe).

For the majority of these identified building damages, specifically those damages located outside of the main urban extent of Tskhinvali, it was generally possible to attribute the damage to a specific military force, with a limited risk of conflating these damages with those resulting from different military forces. The arson-related building damages concentrated to the north and east of Tskhinvali were confidently attributed to South Ossetian militias engaged in a widespread campaign to cleanse the region of ethnic Georgian residents.

Considering the scale and prolonged nature of the arson attacks over the course of a ten-day period, there was at least a prima facie case that the Russians, as

continued active fires in the villages were detected on 22 August 2008, it is likely that there were more than 300 damaged buildings in the four ethnic Georgian villages to the east of Tskhinvali (from Pirsi to Eerie).

the occupying power of South Ossetia[28] at the time, had systematically failed to restrain the militias from attacks against civilians and residential property, and were therefore responsible for serious violations of multiple Articles in the Fourth Geneva Convention.[29]

Because of the recognized complexity of the ground-fighting between Georgian and Russian/South Ossetian forces in Tskhinvali between 7 and 12 August, it was apparent that a satellite-based damage assessment within the city posed significant technical and political challenges in terms of both accuracy and potential force attribution. The preliminary assessment for the city was based on the imagery acquired on 19 August 2008, and identified a total of 230 affected buildings. Of this total, 175 buildings were completely destroyed and a further fifty-five severely damaged.[30] The damages were distributed in a roughly uniform pattern across the city, with multiple small pockets of near total destruction, the worst being the old Jewish quarter of the city with more than twenty-five destroyed buildings in close proximity.[31]

While review of the damage signatures identified in the imagery strongly suggested that most were probably the result of artillery fire, the distinct clusters of building destruction were more consistent with damage patterns typically resulting from a barrage of Grad rockets.[32] Despite the competing denials of responsibility for the reported residential building damages, imagery assessment suggested that a prima facie case existed against Georgian forces for the indiscriminate use of heavy artillery, and specifically Grad rockets, against densely populated areas of the city during their offensive to capture Tskhinvali on the morning of 8 August 2008.

Based on the findings of post-conflict field validations in Lebanon in 2006,[33] which showed increasing errors of omission for less severe forms of building damages, it was assumed at the time of the initial assessment that building damages were likely to have been underestimated within the urban environment of Tskhinvali. However, what was poorly understood during the assessment of Tskhinvali was the potential magnitude of the underestimation of severe building damages resulting from tank and artillery shells fired at close range into the sides of buildings.

In September 2008 a Russian NGO, Charta Caucasica, based in the republic of North Ossetia later posted a critical review of the UN satellite-based damage

28 Report of Independent International Fact Finding Mission on the Conflict in Georgia (IIFFMCG), Council of the European Union, 2009, paras. 19–28, available at: http://www.ceiig.ch/pdf/IIFFMCG_Volume_I.pdf (last visited June 2012).

29 Based on the imagery recorded on 19 August, multiple concentrations of Russian main battle tanks and assorted heavy transport vehicles were identified in villages north of Tskhinvali at the time arson attacks were occurring, strongly suggesting that Russian forces had passively supported the Ossetian campaign of looting and destruction against ethnic Georgian villages and property.

30 Damage figures from initial UNOSAT assessment completed on 22 August 2008.

31 See field report of Jewish Quarter destruction in Catherine Belton, 'Tskhinvali bears scars of military maelstrom', in *The Financial Times*, 18 August 2008, available at: http://www.ft.com/cms/s/0/06946f30-6cbb-11dd-96dc-0000779fd18c.html#axzz1tedp35Eb (last visited 10 April 2012).

32 Based on author's internal UN correspondence.

33 Internal field validation commissioned by UNITAR/UNOSAT in southern and eastern areas of Lebanon following the conflict with Israel, September–October 2006.

assessment for Tskhinvali. Based on a basic ground survey of the city, the NGO graphically documented the location and type of damages that the UN assessment had failed to identify. Although their critical ground survey was neither rigorous nor did it attempt to provide statistical estimates for errors of omission and commission, the observations in it nevertheless strongly suggested that overall building damages in the city had been seriously underestimated because of the generalized failure to identify from the available imagery the artillery and rocket fire into the sides of mostly residential high-rise buildings.[34]

Ground photos of buildings with clearly defined side-impact craters and blast marks were presented with annotated clips of the relevant building as marked in the UN satellite image maps. Figures 5 and 6 show the exact location of unidentified damaged buildings as located in the imagery and the associated photos of the same location taken from the ground. The general conclusion of Charta Caucasica was that satellite imagery was poorly suited for accurate assessment of the full range of damage within the city because of the limited view angle and spatial resolution of the sensor used.[35] These important limitations should have been better understood and anticipated, and that more explicit disclaimers and qualifications should have been included in the maps produced.

Sri Lanka (2009)

Satellite analysis work conducted by the UN during the Sri Lankan civil war was initiated following a direct request in January 2009 from the UN Country Team in Colombo to provide population estimates of internally displaced Tamil civilians trapped within the government declared No Fire Zones (NFZ-1, -2 or -3) in Mullaittivu district.[36] Satellite imagery was also collected and analysed during the final five months of the conflict to provide monitoring of large-scale civilian movements, to assess reported shelling incidents within the NFZs, and to identify building damages and impact craters from artillery fire and air strikes. Because of the political sensitivity of the negotiations between the UN Country Team and Sri Lankan authorities over humanitarian access to the conflict zone, satellite-derived reports were not released publicly. However, the Sri Lankan government was duly informed of both their production at the time and the general findings of the analysis during the course of negotiations.[37]

A second phase of analysis was conducted in direct support of the UN Secretary General's Panel of Experts on Sri Lanka in 2010 (the Panel).[38] Using an

34 Available at: http://www.caucasica.org/analytics/detail.php?ID=1387 (last visited 29 April 2012).
35 *Ibid.*
36 Project work conducted by UNITAR/UNOSAT in 2009.
37 The leak of one report by a foreign Embassy to the UK media and the subsequent accidental release of a second report, both in April 2009, provoked a small diplomatic crisis provoking the Sri Lankan government to accuse the UN of 'spying'. See interpretation from US Embassy cable, available at: http://wikileaks.org/cable/2009/05/09COLOMBO484.html# (last visited 4 May 2012).
38 Report of the Secretary-General's Panel of Experts on Accountability in Sri Lanka, UN Doc. 31 March 2011, para. 127, available at: http://www.un.org/News/dh/infocus/Sri_Lanka/POE_Report_Full.pdf (last visited June 2012).

Figure 5: Ground photo of damaged building with side impact crater, Tskhinvali (September 2008), (photograph courtesy of NGO Caucasica).

approach similar to that used by the Goldstone Mission on Gaza, the Panel drew upon the analysis of satellite imagery for corroboration of individual testimonies related to the shelling of protected sites. The Panel also looked to the imagery analysis to provide, when possible, primary analysis on force attribution for the shelling of areas within the NFZs that were populated with thousands of civilians at the time.

Additional analytical work was conducted on air strike locations and targeting by the Sri Lankan air force, as well as the projected fire bearings of Sri Lankan army mortar and heavy artillery batteries in relation to documented zones of indiscriminate shelling. The analysis findings were presented to the Panel in the form of multiple briefings as well as a finished report,[39] which was partially incorporated into the Panel's final report to the Secretary General, released in March 2011.[40]

39 'Geospatial Analysis in Support to the Secretary-General's Panel of Experts on Sri Lanka', unreleased UN Doc, 17 January 2011.

40 Report of the Secretary-General's Panel of Experts, above note 38.

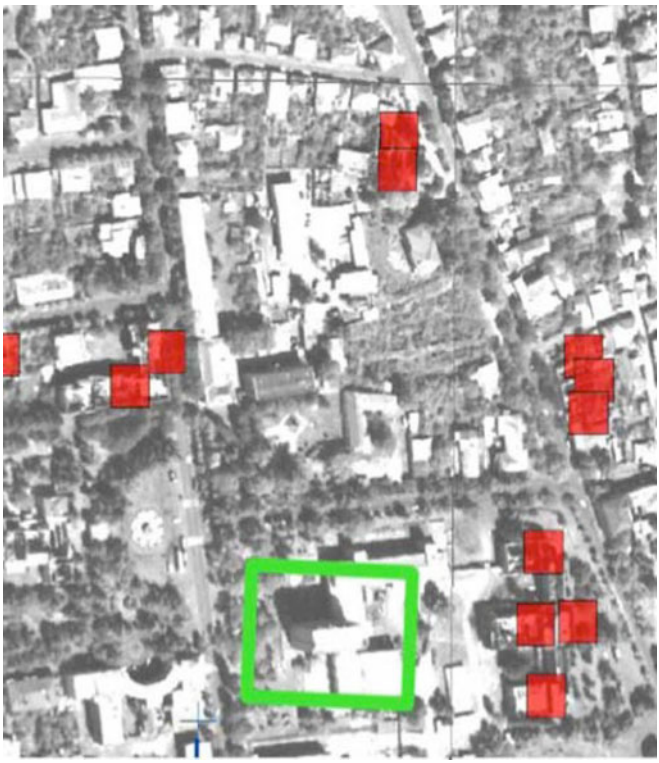


Figure 6: Satellite map of building shown in Figure 5 (marked in green) surrounded by building damages identified from the imagery (marked in red) (UNITAR/UNOSAT) (Image © DigitalGlobe).

The Panel was primarily interested in detailed damage assessments for a list of protected medical and humanitarian facilities within the conflict zone, both to confirm the dates of reported artillery shelling, and to determine attribution for the attacks if possible. Of the ten specific medical, humanitarian, and religious facilities examined for the Panel,[41] each showed clear indications of severe building damages probably resulting from indirect artillery fire. Further, the seven medical facilities and the UN humanitarian aid centre were apparently subject to artillery fire while they were reportedly still operational and occupied by civilians seeking humanitarian assistance.

Damage identified within the satellite imagery ranged from small impact craters on building roofs and open courtyards, to instances of total building collapse. All the sites reviewed were either clearly marked as protected humanitarian sites

41 These facilities were seven hospitals, the UN distribution centre, and two cultural/religious sites (New Housing Colony Kandaswamy Temple in PTK, and Kumara Kanapathi Pillaiyar temple in Mullivaykkal West division, NFZ-2).

Figure 7: Satellite-based damage assessment for Vallipunam hospital, Sri Lanka (UNITAR/UNOSAT).

with rooftop medical insignia visible from the air,[42] or easily distinguished as protected cultural sites by the distinctive building architecture. As shown in Figure 7, the assessment provided to the Panel of the damage to the Vallipunam hospital located on the southern edge of the first NFZ-1 clearly indicated the compound had been heavily damaged by artillery shelling and on multiple dates.[43]

With respect to the question of attribution, although there was little doubt that the protected sites reviewed had been damaged by repeated artillery shelling, there was in fact no signature evidence that would have enabled determination of responsibility for the damage, let alone to address the allegations of deliberate targeting. Such damage signatures left by small- and medium-calibre mortar fire could have conceivably come from either the Tamil Tigers (LTTE) or the Sri Lankan army. This is not to suggest that it was impossible to use the imagery available to attribute damage, only that it was not possible based on the site-specific eyewitness testimonies provided to the Panel.

However, once the scale of assessment was expanded to cover larger areas that encompassed the protected sites it became possible to draw reasoned conclusions about which military force was likely responsible for the attack.

42 The Red Cross symbol was generally easily visible in the commercial satellite imagery used in the report.
43 Assessment maps for the protected sites were included publicly in the Report of the Secretary-General's Panel of Experts, above note 38.

Detailed assessments for areas within the NFZ-1 and the NFZ-2, and the centre of Puthukkudiyiruppu (PTK) identified a total of 1,525 specific damage sites.[44] Of this total, over 200 permanent buildings were either destroyed or severely damaged, with an additional 230 separate impact craters identified on permanent building rooftops, and a further 1,020 impact craters identified on open spaces (i.e. fields, beaches, etc.).

Based on analysis of these larger shelling zones, it was concluded that damages to the specific protected sites were, in fact, not the result of isolated or misdirected artillery fire, but part of much larger shelling events, best characterized as area bombardment. Considering the volume of munitions deployed over such large areas and the depleted state of LTTE forces, there was little doubt that only the Sri Lankan army was capable of such heavy and sustained artillery fire. Detailed maps and quantitative figures on these shelling zones were presented to the Panel for consideration as compelling cases of indiscriminate and disproportionate military force by the Sri Lankan army in areas densely populated with tens of thousands of displaced Tamil civilians.[45]

A detailed review of probable air-strike-related damages during a five-month period identified over 130 separate locations directly attributable to the Sri Lanka Air Force (SLAF).[46] A significant majority of these air strikes were directed against locations with indications of recent LTTE activity,[47] outside designated NFZs, and removed from concentrations of civilian tents. There were, nevertheless, over ten specific air strike impact craters identified immediately adjacent to civilian tent concentrations and a functioning hospital. One particular air strike location identified inside the NFZ-2 was documented at the time in an internal UN report completed on 2 April 2009,[48] and represented the first independent evidence of government air strikes within the NFZ-2 contrary to an explicit prohibition against, and denial of, such attacks by the Sri Lankan government.[49] This report was obtained by a journalist in Colombo who broadcast a story, discussing the main findings of the report, for Channel 4 ITN (UK) on 21 April 2009. The fact that Sri Lankan authorities did not issue any comment

44 Defined as individual impact craters located on building roofs, open fields, wetlands, and roads, as well as permanent buildings that show damage signatures more severe than limited rooftop impact craters (i.e. partial or total destruction).

45 'Geospatial analysis', above note 39.

46 There was no remaining LTTE air force by late January 2009.

47 Specific site examples included the construction of defensive earthen berms and trenches, building activity immediately adjacent to thick tree-cover near the front line, visible troop formations along roads and beaches, and small boats partially buried on beaches.

48 Satellite-Detected Damages and IDP shelter Movement Report for March 2009, internal UN distribution, 2 April 2009. It was noted in the report that the air strike location identified was within a section of the NFZ-2 without visible civilian tent shelters.

49 'Sri Lanka admits bombing safe zone', in *Al-Jazeera*, 2 May 2009, available at: http://english.aljazeera.net/news/asia/2009/05/20095141557222873.html (last visited 3 May 2012).

following the broadcast was interpreted at the time as a tacit validation of the report conclusions.[50]

An important contribution to the Panel's investigation was a detailed analysis of Sri Lankan artillery batteries located throughout the conflict zone. By monitoring the positioning and orientation of the howitzers and mortar pits over time, it was possible to observe that the Sri Lankan army repeatedly rotated the fire bearing of their artillery towards the NFZ-2 and later the NFZ-3, tracking the movements of civilians and LTTE forces alike as they were forced into the southern sections of a barrier island in late April and early May 2009. These findings were presented to the Panel as compelling evidence that the Sri Lanka Army had, throughout the last months of the conflict, established, maintained, and updated an operational military capability to direct substantial quantities of artillery fire into these NFZs that were heavily populated with civilians at the time.[51]

As illustrated in Figure 8, there were also documented cases in which the Sri Lanka Army erected artillery batteries on the grounds of a primary school and the main PTK hospital.[52]

In contrast to Gaza, where no meaningful evidence was produced on potential violations of IHL committed by Hamas during the conflict, there was a significant, if incomplete, body of compelling evidence against the Tamil Tigers during the final stages of the civil war. Not only was it possible to identify cases where the LTTE had tactically deployed artillery next to civilians, apparently using them as human shields – a war crime – it was also possible to document the LTTE's repeated construction of military fortifications (mostly earthen berms and trenches) adjacent to medical facilities, religious sites, and other shelters filled with civilians in violation of international law by putting civilians at unnecessary risk of military attacks by the Sri Lankan armed forces.

The most compelling and comprehensive evidence compiled against the LTTE involved their deliberate positioning of hundreds of heavy vehicles suspected of containing military equipment within areas densely populated by civilians, effectively using them as a human shield against potential attack, as well as exposing civilians to the potential ignition of the vehicle contents. At the end of the conflict, LTTE heavy vehicles were involved in a massive explosive event on the morning of 16 May 2009, producing a zone of total incineration measuring approximately 36,000 m^2 in area and destroying an estimated 200 tent shelters. Because of uncertainty about the estimated civilian population remaining within the NFZ-3 at the time, it was not possible to estimate the potential civilian deaths or injuries resulting from the explosion.[53]

50 Video available at: http://link.brightcove.com/services/player/bcpid1529573111?bclid=20223644001&bctid=20379565001 (last visited 3 May 2012).

51 See artillery time series analysis maps in Annex: Report of the Secretary-General's Panel of Experts, above note 38.

52 It is unlikely that either of these public facilities was functioning at the time; however, the school was later demolished and as of late 2010 there were no indications that the hospital had been reconstructed.

53 This explosion was detected by the same fire-monitoring sensors used during the Georgian conflict (2008).

Figure 8: PTK hospital (partially destroyed) with Sri Lankan army mortar battery visible on hospital grounds in lower left (17 June 2009) (Image © GeoEye).

Satellites to the rescue?

As shown through the three case studies of Gaza, Georgia, and Sri Lanka, analysis of satellite imagery can often provide independent and compelling evidence in direct support of war crimes investigations. There are, however, a range of technical limits, analytical challenges, and political restrictions to the application of imagery for IHL which must be better understood in order to properly manage expectations of this exciting field of applied humanitarian research.

Technological limits

The obvious limitation of electro-optical satellite sensors is that they simply cannot see through clouds, dense tree-cover, or at night, thereby geographically and seasonally limiting their ability to assess or monitor armed conflicts in many regions of the world. Had the final months of the Sri Lanka civil war occurred, for example, during the eastern monsoon season in late 2008 rather than during the dry season in early 2009, sustained cloud cover would have prevented the use of electro-optical sensors to provide detailed analysis of the conflict.

An increasingly viable alternative source of satellite data in such circumstances is the new generation of radar sensors (known as synthetic aperture radar or SAR sensors) that do not have the same weather-based limitations as standard electro-optical sensors. Because SAR sensors actively map or illuminate the ground using radar, the derived data can be easily acquired at night, through heavy clouds, and even, under certain circumstances, through dense vegetation. Relevant investigative applications could include, for exaample, identifying areas of significant building damages and conflict-related environmental impacts and locating large concentrations of displaced civilians both on land and sea,[54] as well as the monitoring of conventional military forces.[55] Despite these important advantages in capability, the practical application of SAR data for research by civilian institutions and NGOs on potential violations of IHL has been limited by several important factors. Traditional image interpretation and processing methods commonly used with electro-optical imagery are not easily transferred to analytical work with SAR data because of the complexity of radar signatures. Analysts possessing such specialized skills are still heavily concentrated within national military and intelligence agencies and thus less available for equivalent civilian research. Because of the often dual-use legal agreement underpinning the operation of very high resolution SAR sensors, there are not only significantly higher data costs, but the data is also potentially subject to political restrictions over sensitive areas.[56]

One poorly understood but frequently encountered limitation is that very high resolution (VHR) satellites (including both electro-optical and SAR sensors) do not collect imagery automatically and continuously over the world, but rather are tasked over specific areas with known commercial, political, or humanitarian value.

54 SAR sensors are especially well suited for monitoring vessel traffic on open bodies of water, which would be of specific value to detailed studies on potential human-trafficking routes, as well as large-scale forced population displacements by boat.

55 Rob Dekker, *et al.*, 'Change detection tools', in Bhupendra Jasani, *et al.*, (eds), *Remote Sensing from Space – Supporting International Peace and Security*, Springer, 2007, pp. 119–140.

56 The German SAR sensor TerraSAR-X is subject to the Satellite Data Security Act (SatDSiG) of 2007, which restricts civilian access to radar data collected over designated sensitive areas. It is not known at the time of writing to what extent in practice this policy has actually restricted data access over conflict zones. See 'German national data security policy for space-based earth remote sensing systems', 2010, available at: http://www.oosa.unvienna.org/pdf/pres/lsc2010/tech-02.pdf (last visited June 2012). See also 'PPP between DLR and Infoterra the SatDSiG – German Satellite Data Security Act', 2008, available at: http://www.gwu.edu/~spi/assets/docs/PPP_DLR_SatDSiG-Datenpolicy_Bernhard.pdf (last visited June 2012).

This can mean that unreported and unanticipated conflicts in remote areas can easily go undocumented by commercial sensors for weeks or months at a time, leaving little or no relevant evidence of the conflict detectable in the available imagery once it is eventually acquired. There were, in fact, multiple instances encountered by the UN over the last five years in which requests for satellite-based analysis of particular incidents were simply never conducted for lack of relevant imagery coverage.[57]

Asymmetrical conflicts involving irregular forces, as in Gaza and Sri Lanka, will continue to present serious technical and analytical challenges. Because of limits to the resolution of civilian satellite sensors, it will remain exceedingly difficult to identify the movement or actions of irregular or poorly-armed insurgent groups, groups which do not possess or are not in a position to deploy conventional military forces and materials readily identified from space. Small-unit guerrilla forces fighting within urban environments or under camouflage or dense vegetation canopy will remain largely invisible, posing a general problem of unbalanced focus on the actions of conventional armed forces.[58]

Satellite imagery analysis will continue to be limited in its ability to identify the use of prohibited weapons systems. In Georgia, for example, no meaningful evidence on the use of cluster munitions by Russian forces in and around the city of Gori was collected from imagery despite detailed field reports from Human Rights Watch providing the approximate timing and locations of the reported attacks.[59] Basic questions regarding the use of white phosphorus artillery shells in Gaza by the IDF could not be answered for lack of signatures in the imagery, and thus no insights on the potential legality of their use were possible.

One of the most serious limitations to conducting satellite-based damage assessments remains a chronic inability to detect damages caused by ground fire from tanks, rocket-propelled grenades and low-trajectory artillery. In the case of Tskhinvali, this resulted in an undercount of potentially hundreds of affected building sites across the city, leading to the risk of a perception of political bias against South Ossetian forces simply because the arson-related damages they inflicted were more easily and accurately documented. It would be safe to conclude that the damage assessment maps released by the UN at the time contained uneven levels of accuracy, with errors of omission spatially concentrated in exactly those

57 Based on the author's experience at UNITAR/UNOSAT (2005–2012).

58 The only information collected in relation to potentially unlawful acts in Gaza by Hamas was the identification and analysis by UNOSAT of damage to the retaining wall of a sewage treatment plant that resulted in a massive outflow event over 1.2 km long. The Goldstone Report assumed Israeli forces had been responsible; however, there were no eyewitnesses and little physical evidence. The Israeli government reviewed the case and concluded that although they could not rule out an accidental air strike, they thought it could have been committed by Hamas as part of a defensive plan to hamper the movement of IDF tank forces in the area. If this were the case then it would potentially represent a violation of customary international law as reflected in Article 56 of Protocol I and Article 15 of Protocol II, prohibiting the destruction of installations containing dangerous forces. See 'Gaza operation investigations: an update', in *Israeli Ministry of Foreign Affairs*, January 2010, paras. 150–164, available at: http://www.mfa.gov.il/NR/rdonlyres/8E841A98-1755-413D-A1D2-8B30F64022BE/0/GazaOperationInvestigationsUpdate.pdf (last visited 1 May 2012).

59 Based on the author's internal UN correspondence with Human Rights Watch, August–September 2009.

parts of the city that had been most affected by Georgian government shelling during their offensive in early August 2008. Unfortunately, it is unlikely that this specific limitation will be adequately addressed in the near future despite anticipated improvements in sensor technology.

Analytical challenges: ambiguous, inconclusive, and uncertain findings

It is important to understand that detailed imagery analysis can often result in ambiguous, inconclusive, and even politically contested or erroneous findings. An example is the largely discredited interpretations of satellite imagery presented by US Secretary of State Powell at the UN Security Council over alleged chemical and biological weapon facilities in Iraq during the build-up to the Second Gulf War.[60] Analysts can make mistakes, come to widely divergent conclusions about the same image, and can even subconsciously shape their findings to meet preconceived user or organisational expectations. More common are a broader range of circumstances when complex events occur on the ground and present distinct challenges for the production of relevant and meaningful satellite-derived information on armed conflict.

One of the primary challenges encountered during the Sri Lankan civil war was the difficulty confirming reports of mortar shelling within the NFZs – clearly an issue of acute relevance to the Panel of Experts' investigation. Survival tactics such as the construction of family wells, latrines, and bomb shelters, as well as the high portability of tents and the associated debris left behind, had the cumulative effect of substantially masking the impact signatures of small- and medium-calibre mortar shells. It was therefore likely that evidence of artillery shelling was differentially masked in areas, depending on the relative number of civilian tent shelters, effectively leaving areas of highest population density with the lowest levels of shelling evidence.

Uncertainties in image interpretation are commonly encountered in complex or unfamiliar environments when the temporal coverage of available imagery is insufficient to capture and reconstruct a series of specific events on the ground. Multiple interpretations, each of which is potentially equally probable, may result in such circumstances, leaving questions of direct humanitarian interest unanswered. Typically ambiguous cause-and-effect scenarios result from the binary comparison of two satellite images recorded over a given area, one recorded before an event and the other after. The objective in this context is to try to determine exactly what occurred on the ground between these two static snapshots in time.

60 The 2004 US Senate report on US pre-war intelligence on Iraq indicated that when imagery analysts came to strongly divergent opinions about the significance of vehicle activity at the Amiriyah Serum and Vaccine Institute, there was no mechanism or review process to resolve the conflict, allowing the erroneous interpretation of 'unusual' activity to go into the Powel presentation. Further, it appears that imagery analysts may have shaped their findings on the locations of alleged mobile biological weapons (BW) agent production units to conform to fabricated reports by the informant 'Curve Ball'. See 'Report on the US Intelligence Community's Prewar Intelligence Assessments on Iraq', US Senate, 7 July 2004, pp. 244–256, available at: http://web.mit.edu/simsong/www/iraqreport2-textunder.pdf (last visited June 2012).

When analysis is dependent on a very limited time series of imagery, especially when the 'pre-imagery' is recorded months or sometimes even years before, it is probable that multiple complex events will effectively be compressed into one static and highly ambiguous overview which is of little value.

A basic question asked of satellite imagery after reports of rebel forces advancing on a refugee camp, for example, is has the camp been attacked or not? Although the post-event image may indeed show the absence of tent shelters, it may not necessarily contain enough details to determine with sufficient confidence whether rebel forces demolished the shelters during an attack, or if the shelters were hurriedly packed by fleeing residents in advance of a feared attack. In such complex and poorly documented circumstances, the relative lack of sufficient satellite imagery will usually result in ambiguous and inconclusive findings.[61]

As is apparent in all three of the case studies, determining likely force attribution for any given attack based on a narrow inspection of damage signatures contained in available imagery is often exceedingly difficult and potentially misleading. For example, small impact craters identified on hospital rooftops or in open fields in Sri Lanka could, if taken in isolation from the wider context, conceivably have been inflicted by either side in the conflict. Even large-scale events, such as the massive explosion during the final hours of the Sri Lankan civil war, may present ambiguous or marginal clues within the imagery insufficient to suggest which side was likely responsible.

Political restrictions and the future

Since the US government decision in 1994 to authorize the commercialization of essentially military technology, public access to very high resolution satellite imagery and the proliferation of new and improved sensors has generally proceeded without significant political interference or restrictions.[62] There remains, however, a notable exception that continues to adversely impact the use of imagery over important conflict areas in the Middle East. In 1997 the US government enacted a law prohibiting the sale or distribution of satellite imagery with under two metre spatial resolution over Israel, Gaza, the West Bank, the Golan Heights, as well as within a five-kilometre buffer zone into Egypt, Syria, and Lebanon.[63]

This restriction was directly felt during the Gaza conflict in 2009, in that it forced commercial satellite providers to systematically degrade imagery recorded over the Gaza Strip to only 25 per cent of the original resolution. In fact, all of the UN monitoring and analysis work on Gaza for the humanitarian community, and specifically for the Goldstone Mission, was based on degraded-quality imagery that

61 A clearly associated risk with the proliferation of satellite imagery use by the humanitarian and NGO community is that groups may release products out of inexperience, excitement, or pressure to confirm preconceived expectations that do not necessarily account for this uncertainty or fully communicate it to end users, risking a typical rush to judgement error, as exemplified by the presentation of satellite imagery interpretations by then US Secretary of State Colin Powell at the UN Security Council in February 2003.

62 See Y. A. Dehqanzada and A. M. Florini, above note 1.

63 National Defence Authorisation Act for Fiscal Year 1997, US Government, 23 September 1996, Sec. 1064.

had a significantly negative impact on overall accuracy and confidence levels. Although no attempts have been made to quantify the impact, it almost certainly caused a systematic underestimation of virtually all forms of building and infrastructure damage across the Gaza Strip.

Although legally this restriction applies only to US satellite sensors, both the US and Israeli governments have, until recently, successfully secured bilateral agreements with European and Asian satellite companies to adopt similar restrictions.[64] One apparent consequence of recent diplomatic tensions between Turkey and Israel is that the planned Turkish satellites GökTürk-1 and GökTürk-2 may start by 2013 to acquire and distribute sub-metre resolution imagery over the whole of Israel and the Palestinian territories.[65] If this occurs, it could conceivable lead to the eventual revision or outright repeal of the US restriction.

One of the potential political consequences of the use of satellite technology for conflict monitoring and analysis is a growing interest of many UN member states within the Group of 77 to restrict the production and public release of satellite-based research on pressing issues of human rights and IHL. Programmes within the UN system have, in fact, come under pressure from recent agency guidelines that are increasingly restricting the public dissemination of satellite-derived information on armed conflicts and major humanitarian emergencies.[66]

It remains uncertain if these political attempts within the UN system to restrict the use of satellite technology will have a long-term negative impact on the ability of the UN to support future investigations. What is certain, however, is that in the near future the broader humanitarian and human rights community will increasingly adopt the necessary technical and analytical skills in order to conduct their own independent satellite-based conflict monitoring and analysis.

64 'Turkey dismisses Israel's concerns over satellite', in *Reuters*, 11 March 2011, available at: http://www.reuters.com/article/2011/03/11/turkey-israel-satellites-idUSLDE72A1VM20110311. See also 'Göktürk – project of reconnaissance and surveillance satellite system', Turkish Air Force, available at: http://www.hvkk.tsk.tr/EN/IcerikDetay.aspx?ID=167&IcerikID=154 (both last visited 5 May 2012).

65 *Ibid.*

66 Based on internal UN correspondence and private discussions with UN colleagues (2005–2012).

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

The roles of civil society in the development of standards around new weapons and other technologies of warfare

Brian Rappert, Richard Moyes, Anna Crowe, and Thomas Nash

Brian Rappert is a Professor of Science, Technology and Public Affairs in the Department of Sociology and Philosophy at the University of Exeter. His latest book, *How to Look Good in a War*,* examines how secrecy and transparency, as well as knowledge and ignorance, mix and meld together in the practice of statecraft.

Richard Moyes is Managing Partner of the UK non-governmental organization Article 36 and is an Honorary University Fellow at the University of Exeter.

Anna Crowe recently completed her Master of Laws at Harvard Law School. She previously worked as a New Zealand government lawyer and prior to that as a clerk to the Chief Justice of New Zealand.

Thomas Nash is Director of the UK non-governmental organization Article 36. He coordinated the Cluster Munition Coalition, the international campaign that led to the 2008 treaty banning cluster munitions.

* Brian Rappert, *How to Look Good in a War. Justifying and Challenging State Violence*, Pluto Press, London, 2012.

doi:10.1017/S1816383112000744

Abstract

This article considers the role of civil society in the development of new standards around weapons. The broad but informal roles that civil society has undertaken are contrasted with the relatively narrow review mechanisms adopted by states in fulfilment of their legal obligations. Such review mechanisms are also considered in the context of wider thinking about processes by which society considers new technologies that may be adopted into the public sphere. The article concludes that formalized review mechanisms, such as those undertaken in terms of Article 36 of Additional Protocol I (1977) of the Geneva Conventions of 1949, should be a focus of civil society attention in their own right as part of efforts to strengthen standard-setting in relation to emerging military technologies.

Keywords: weapon review, Article 36, civil society, new technology.

It is widely accepted that humanitarian and moral considerations should constrain the choice of tools with which people can legitimately kill and injure each other. International humanitarian law (IHL) – in the form of treaties and customary international law[1] – codifies this belief in relation to armed conflict by requiring a balance between the need for military necessity and concerns for 'humanity'.[2] This requirement for a balancing is expressed in a number of specific legal rules, such as those regarding superfluous injury and unnecessary suffering, indiscriminate attacks, and proportionality.[3] However, it is an open question whether this framework is sufficient to limit effectively the harm caused by weapons.

The starting point for this article is that determining the acceptability or otherwise of weapon technologies presents numerous challenges and difficulties. As a matter of principle, defining what is illegitimate is inextricably tied to affirming what means and methods for killing and injuring are legitimate. As a result, attempts to restrict particular technologies may be seen as unintentionally sanctioning other forms of violence or even providing tacit acceptance of wider patterns of conflict.[4] Such risks cannot be easily dismissed. Just how expert technical

1 See Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law*, Cambridge University Press, Cambridge, 2005.

2 See Theodor Meron, 'The Martens Clause, principles of humanity, and dictates of public conscience', in *The American Journal of International Law*, Vol. 94, No. 1, 2000, pp. 78–89.

3 See, for example, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 35(2) (superfluous injury or unnecessary suffering), Article 51(4) (indiscriminate attacks) and Article 51(5)(b) (proportionality); see also, International Committee of the Red Cross (ICRC), *Existing Principles and Rules of International Humanitarian Law Applicable to Munitions that May Become Explosive Remnants of War*, Paper Submitted to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, CCW/GGE/XI/WG.1/WP.7, 28 July 2005.

4 For a discussion of this point, see Richard Falk, 'The challenges of biological weaponry', in Susan Wright (ed.), *Biological Warfare and Disarmament*, Rowman & Littlefield, London, 2001; Yves Sandoz, 'Preface', in Eric Prokosch, *The Technology of Killing: A Military and Political History of Antipersonnel Weapons*, Zed, London, 1995; Thomas W. Smith, 'The new law of war: legitimizing hi-tech and infrastructural violence', in *International Studies Quarterly*, Vol. 46, 2002, pp. 355–374.

analysis, appeals to morality, pragmatism, and political power ought to mix together in defining the bounds of legitimacy has no simple solution.

As a matter of practice, doubts can be raised about how humanity and military necessity were balanced in the past. The continuing level of casualties inflicted on non-combatants during and after armed conflict testifies to the limitations of IHL. Historically, where weapon types have already been developed and widely deployed, it has taken a considerable effort to put in place any such constraints subsequently, and in some cases controls have not been devised despite high-level statements that they are necessary.[5]

The process of setting moral standards to limit the means and methods of warfare faces many of the problems that confound decision-making about technology more widely. The high and irreversible costs of damage to humans and the environment, the complexity of operational situations, and the potential lag between harm and attempts to correct it all challenge efforts to minimize negative consequences.[6] Authors such as Morone and Woodhouse have offered a number of suggestions for coping with the difficulties of technology in general.[7] These include putting in place so-called precautionary measures[8] (such as initially limiting use, protecting against severe risks, testing concerns) and building in flexibility (by reducing major uncertainties and learning from experience). In relation to weapons technologies, as elsewhere, such efforts often prove difficult to undertake as careers of individuals, strategies of institutions, organizational structures, and beliefs become moulded around the technologies in question. The desire of states to achieve military advantage, and of companies to achieve commercial gain, all bear against flexibility and transparency.

The pace of weapons development and deployment, driven by technological changes, also challenges the assessment of the implications of new weapons, means, or methods of violence as a matter of public policy. As new mechanisms of applying force become available – whether in the form of autonomous military

5 For example, nuclear weapons are not subject to an explicit legal prohibition against their use despite widespread recognition that such weapons should be abolished. In December 1994, the UN General Assembly requested the International Court of Justice to offer an advisory opinion on the question: 'Is the threat or use of nuclear weapons in any circumstance permitted under international law?' To the central issue of permissibility of nuclear weapons, by a vote of seven to seven decided through the second vote of the President of the Court, the judges ruled that: 'The threat or use of nuclear weapons would generally be contrary to the rules of international law applicable in armed conflict, and in particular the principles and rules of humanitarian law. However, in view of the current state of international law, and of the elements of fact at its disposal, the Court cannot conclude definitively whether the threat or use of nuclear weapons would be lawful or unlawful in an extreme circumstance of self-defence, in which the very survival of a State would be at stake. So while the threat or use of nuclear weapons was *generally* held to be against international law, the judges could not determine that it *always* would be. Just as what would constitute "the very survival of a State" was not defined. In many respects, the decision could be characterized as a decision not to decide, at least not to determine once-and-for-all the matter of legality'. See International Court of Justice (ICJ), *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion of 8 July 1996, ICJ Reports 1996, p. 266.

6 Edward J. Woodhouse, 'Is large-scale military R&D defensible theoretically?', in *Science, Technology, and Human Values*, Vol. 15, No. 4, 1990, pp. 442–460.

7 Joseph Morone and Edward Woodhouse, *Averting Catastrophe*, University of California, Berkeley, 1986.

8 Precaution in this usage being aligned with forms of general risk reduction, rather than relating to precaution as specified under the provisions of IHL.

robots, software capable of disabling infrastructure relied on by society, or directed energy weapons – it is unclear that there are either formal or informal mechanisms in place to ensure that the technologies adopted accord with widespread conceptions of what is right or wrong. This may be further complicated where technological changes occur incrementally, making it more difficult to identify or construct categorical 'boundaries'. If concerns about new technologies gain traction in public discourse, efforts will need to be made to ensure that such concerns do not, at the same time, serve to further normalize means and methods of warfare that are currently employed, but in urgent need of further controls.

The purpose of this article is to assess the possible contribution of civil society, as a diverse body of international and national non-governmental actors, in the development of normative standards around new weapons and technologies of warfare and to raise questions about that role in the context of the obligations and duties of states. The first section surveys important functions that can be fulfilled by civil society organizations. By drawing on past and prospective controversies associated with specific weapons, it sets out the need for, potential for, and challenges with civil society contributions. The second section then examines one area in detail: the formal national review of weapons required by Article 36 of Additional Protocol I to the Geneva Conventions of 1949. The final section offers closing reflections.

The roles of civil society

Setting standards about weapons and other technologies of warfare is both demanding and open to question. The general practice of states has been to limit decision-making about such standards to a tight coterie of government, military, and commercial officials, who engage in wider international discussion where such a forum is provided. While this approach favours military and commercial secrecy it is likely to seriously limit the capacities, competences, and concerns informing the setting policy. Nonetheless, in recent years, civil society working in partnership with like-minded states and international organizations has had a prominent role in developing stronger legal controls over certain types of weapons.[9] This has been most notable in the development of prohibitions on anti-personnel landmines (1997)[10] and cluster munitions (2008).[11] Such achievements are formal manifestations of wider ongoing work by civil society in relation to weapons and violence. That said, moving from the identification of concerns to influential action typically requires a substantial investment of time and energy. But non-governmental organizations and others in civil society often have limited capacities in terms of

9 This article does not analyse the concept of 'civil society' in detail, but we use the term primarily to refer to non-governmental organizations, working together or in coalitions, to promote reductions in harm through reforms in practice, policy, or law.

10 Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction, 18 September 1997.

11 Convention on Cluster Munitions, 30 May 2008.

people and funding, and even more so in low-income countries. While civil society has functioned as a part of an informal international system of standard-setting on certain weapons the fact that civil society needed to play this role raises questions about how effectively states and others execute their duties to constrain conflict and violence.

Civil society's engagement in the development of standards governing specific weapons is not uniform. In the cases of anti-personnel mines and cluster munitions, civil society engagement was characterized by participation of a broad coalition of coordinated non-governmental organization (NGO) partners from different countries.[12] On other weapon issues, such as in the development of legal responses to blinding lasers and explosive remnants of war, civil society engagement was more limited. Those issues were addressed primarily through expert policy engagement in established fora for legal discussion. On nuclear weapon disarmament, by comparison, there has been wide-ranging civil society engagement in different ways and in different fora, but these engagements have not yet resulted in an international agreement to prohibit nuclear weapons. Thus, while controlling weapons is an area where civil society has played an important role, engagement has taken different forms and has achieved different sorts of results.

While different civil society organizations will have different approaches and ethoses, which include views on the proper role of civil society, this article focuses on five key interrelated and broad roles that members of civil society have played with regard to the development of humanitarian standards:

- information gathering
- analysing
- framing
- redefining
- communicating and representing.

The aim of this section is not simply to extol the virtue of such functions, but to critically assess the prospects for what civil society can offer. There are a number of factors, beyond those raised in the introduction section, that can inhibit meaningful engagement.

Information gathering

Data on human and environmental consequences is often central to debates about the legality or wider appropriateness of weapons. By demanding access to state-held information or compiling field data of their own, groups within civil society can identify problems hitherto ignored or they can develop a deeper understanding of problems already identified. Therefore, information gathering can be vital

12 During the process to develop the treaty banning cluster munitions, the Cluster Munition Coalition, for example, was made up of around 400 member organizations in some 100 countries. For a discussion on the role of civil society in this process, see Matthew Bolton and Thomas Nash, 'The role of middle power-NGO coalitions in global policy: the case of the cluster munitions ban', in *Global Policy*, Vol. 1, Issue 2, May 2010.

to initiating consideration of a particular issue, or for the development of arguments around an issue that has already been established.

Even the most basic forms of information relevant to weapons' effects can be contested and problematic. The topic of deaths from armed violence illustrates the importance of information gathering by members of civil society, and the relatively weak practice of states. For example, deaths resulting from the 2003 Iraq War have been a prominent topic of international public concern. With the absence of efforts by parties to the conflict, including the US, the UK, and others, to produce figures on the numbers of civilians killed (indeed with active efforts to remain ignorant about this matter[13]) it has fallen on those in civil society to produce figures. Largely based on the systematic evidence of media accounts, the NGO Iraq Body Count not only produced an accessible listing of direct civilian deaths inflicted since the intervention, but also has been able to break them down by perpetrator and weapons type.[14] During 2011, many of these dynamics of accountability were repeated when NATO initially denied deaths from its aerial campaign in Libya.[15] NGOs monitoring media reports have been able to offer provisional figures about casualties related to weapon types, although recognizing limitations in the sources they have access to.[16]

Such data can be very valuable for making further assertions regarding the role played by certain weapons in the production of civilian harm and often stand in contrast to states' own abilities or willingness to provide such data. Despite decades of public concerns regarding cluster munitions, and repeated assurances that such weapons were acceptable given a 'careful weighing' of military benefits and civilian risks, the UK was unable in 2005 to point to any data that it had gathered on their humanitarian impact.[17]

Given such weaknesses in state practice, a group of NGOs have endorsed a Charter for the Recognition of Every Casualty of Armed Violence, and are initiating an 'Every Casualty Campaign' calling on states to recognize that they have a responsibility to record, identify, and acknowledge all casualties of violence.[18] This initiative builds on recognition that developing controls on deployed weapons is likely to require data regarding harms caused, but that the parties responsible both for using the weapons and establishing such controls rarely produce such data.

However, information gathering raises many questions. 'Information about what?' being one. In relation to civilian harms, the question of which deaths should

13 Brian Rappert, 'States of ignorance: the unmaking and remaking of death tolls', in *Economy and Society*, Vol. 41, No. 1, 2012, pp. 42–63.

14 Madelyn Hsiao-Rei Hicks, *et al.*, 'Violent deaths of Iraqi civilians, 2003–2008: analysis by perpetrator, weapon, time, and location', in *PLoS Medicine*, Vol. 8, No. 2, 2011, pp. 1–15.

15 C. J. Chivers and Eric Schmitt, 'In strikes on Libya by NATO, an unspoken civilian toll', in *New York Times*, 17 December 2011, p. A1.

16 Action On Armed Violence, *Explosive Violence Update: Libya*, AOAV, London, 23 June 2011. Madelyn Hsiao-Rei Hicks, Hamit Dardagan, *et al.*, 'The weapons that kill civilians – deaths of children and non-combatants in Iraq, 2003–2008', in *The New England Journal of Medicine*, 2009, No. 360, pp. 1585–1588.

17 Brian Rappert, *Out of Balance: The UK Government's Efforts to Understand Cluster Munitions and International Humanitarian Law*, Landmine Action, November 2005, available at: http://www.landmineaction.org/resources/Out%20of%20Balance.pdf (last visited 24 April 2012).

18 See, for example: www.oxfordresearchgroup.org.uk/rcac (last visited 21 May 2012).

be counted is of critical significance. Should that include only those killings directly resulting from violence or should the numbers also include indirect deaths stemming from a loss of public infrastructure and access to medical facilities, which may be a major element of the overall harm?[19] Much of the public controversy about the real number of civilian deaths stemming from the Iraq War stemmed from alternative assumptions about what should be measured and misconceptions about what was being measured.[20] Decisions about what information should be gathered are likely to be affected by how a problem is depicted, and those decisions may also serve to shape what arguments can subsequently be made. For new weapons technologies, different types of data may be needed at different stages of a weapon's development.

'Information with what assurance?' is another question. Ruge recounted how the definition of humanitarian problems related to arms control and disarmament – such as the previously prominent claim there were '110 million mines in the ground' – resulted from limited data being extrapolated into fact.[21] Elsewhere, in arguments about the perceived acceptability of certain weapons it has not been unusual for states to challenge methodologies and data produced by NGOs while offering no data of their own.[22] Issues of methodology and rigour may also shape practices and debates that follow.

'Information when?' is a further question of particular significance for assessment of new weapon technologies. In so far as prohibitions on anti-personnel mines and cluster munitions were driven by information gathered on the humanitarian impact of these weapons, it is important to note that this information only became effective after substantial international use of the weapons and high levels of resulting civilian harm. With respect to emerging technologies, data on harm may not be available and so other types of information may be required. For example, while there is little data on the civilian harms caused by new 'sensor fuzed' weapon systems, NGOs such as Landmine Action (now Action on Armed Violence), Austcare (now ActionAid Australia), and Handicap International have called for technical information regarding these weapons so as to better understand the civilian risk.[23] At the other end of the process, civil society organizations also

19 For example, a 2008 report on the Global Burden of Armed Violence noted that indirect conflict deaths, such as from elevated levels of malnutrition, dysentery, or other easily preventable diseases, was substantially greater than conflict deaths directly attributable to violence. See Geneva Declaration Secretariat, *Global Burden of Armed Violence*, 2008, Geneva, executive summary, available at: http://www.genevadeclaration.org/fileadmin/docs/GBAV/GBAV2008-Ex-Summary-English.pdf (last visited 1 May 2012).

20 Brian Rappert, *How to Look Good in a War*, Pluto Press, London, 2012, Chapter 5.

21 Christian H. Ruge, 'Mitigating the effects of armed violence through disarmament: counting the human cost', in J. Borrie and V. Randin (eds), *Disarmament as Humanitarian Action*, UNIDIR, Geneva, 2006, pp. 23–50.

22 B. Rappert, above note 17.

23 Richard Moyes, 'A sensor fuzed solution?', in Landmine Action, *Campaign Newsletter*, issue 13, Autumn 2007. Austcare and Handicap International, 'Sensor-fuzing and SMArt submunitions: An unproven technology?', February 2008, available at: http://www.handicap-international.fr/uploads/tx_basm08experts/Sensor_fuzed_and_SMArt_submunitions_an_unproven_technology_1_.doc (last visited 20 May 2012).

take on substantial information-gathering functions in order to monitor the implementation of agreements adopted to control certain weapons.[24]

Finally, it should be recognized that information does not on its own generate meaning. Whether the effects or technical characteristics being documented show a weapon that causes disproportionate harm or kills and wounds in some unacceptable way is a question that cannot be resolved simply by comparison of data. Some previous efforts to strengthen the international regime for controlling new weapons, such as the ICRC's SIrUS project, have arguably fallen foul of too great an emphasis on the decision-making power of data.[25]

Analysing

Building on the final point above, civil society organizations generally go beyond simply providing data, and seek to forward assessments about the scale and nature of the problems being documented, the links between those problems and the technology of specific weapon types, and what needs to be done in response.[26] However, there are limits to the role of analysis in developing new standards.

Ideally, it might be imagined that choices about the adoption and deployment of weaponry, as with other technologies, might follow a rational set of stages. Operational objectives would be established first; alternative options to meet those objectives would be scrutinized in detail (including with regard to their humanitarian implications); weapons would be deployed; their performance would be systematically monitored and evaluated; and this experience would feed back into a new cycle of examining objectives, options, and performance. However, political theorists examining how choices are made about technology have long questioned whether such rational models are accurate or even desirable as ideals.[27] A central problem is that they place a great weight on analysis, and do not adequately recognize the extent to which information can be ambiguous and may produce divergent views when approached with different preconceptions or motivations.

Even if data regarding the effects of weapons are relatively undisputed the legal framework governing armed conflict alone provides ample opportunities for analyses to diverge. The meaning of the principles and rules of IHL are uncertain and subject to disagreement in major respects. Phrases such as 'incidental loss of life

24 See, *Landmine Monitor* and *Cluster Munition Monitor*, available at: http://www.the-monitor.org/ (last visited 9 May 2012). For a discussion on the role of the Landmine Monitor in reinforcing the international standard against landmines, see Mary Wareham, 'Evidence-based advocacy: civil society monitoring of the Mine Ban Treaty', in Jody Williams, Stephen D. Goose and Mary Wareham (eds), *Banning Landmines: Disarmament, Citizen Diplomacy, and Human Security*, Rowman & Littlefield, Lanham M.D., 2008.

25 See ICRC, *The SIrUS Project: Towards a Determination of Which Weapons Cause 'Superfluous Injury or Unnecessary Suffering'*, Geneva, 1997; for an example of the criticism directed at the SIrUS project, see Major Donna Marie Verchio, 'Just say no! The SIrUS project: well-intentioned, but unnecessary and superfluous', in *The Air Force Law Review*, Vol. 51, 2001, pp. 183–228.

26 As advocated in Robin Coupland, 'The effects of weapons and the Solferino cycle', in *British Medical Journal*, Vol. 319, No. 7214, 1999, pp. 864–865.

27 See Charles Lindblom, 'Still muddling, not yet through', in *Public Administration Review*, Vol. 39, 1979, pp. 517–526; and Arie Rip, Thomas Misa and Johan Schot, *Managing Technology in Society*, Routledge, London, 1995.

or injury to civilians' and 'concrete and direct overall military advantage', for instance, are subject to significantly different interpretations by government officials and legal scholars.[28] Given these differences, the notion that analysis alone could resolve disputes about legality – let alone wider questions about acceptability – is questionable.

Further, the identification of humanitarian implications that need redress is not done through an exhaustive process of analysing the objective harms of all weapons and then agreeing priority topics for action. Officials, NGOs, and others work with assumptions about what concerns matter. For example, the idea of a weapon that kills or injures by blasting pieces of flesh off the victim is generally not considered problematic, because blasting pieces of flesh off people is seen as common in armed conflict. By contrast, horrific injuries from an 'unusual' type of weapon technology (for instance, biological weapons or white phosphorus) may attract far greater attention even if there is a much more extensive pattern of civilian death and injury associated with technologies considered 'normal' or the use of which is somehow seen as 'inevitable'.[29]

The preceding paragraphs are not meant to suggest analysis has no, or only a highly limited, role to play in setting standards. They are intended to indicate that analysis is most likely to be most meaningful when it contributes to ongoing political processes and dialogues. In such circumstances, the 'framing' of the issue in question can perhaps be narrowed down sufficiently to limit divergence of opinion regarding the underpinning terms of the debate. A good example is that of the 2007 report by Norwegian People's Aid in collaboration with the Norwegian Defence Research Establishment regarding the in-field reliability of the M-85 submunition.[30] By directly challenging one of the proposals being debated at the time as part of the Oslo Process on cluster munitions – namely that submunitions with a self-destruct mechanism could sufficiently address humanitarian concerns – the report helped policymakers resolve a choice that was being posed to them.[31]

Framing

Claims about the causes of the problems associated with weapons and what needs to be done about them also speak to issues of framing. Gamson and Modigliani referred to frames as the central ideas for structuring our sense of events and the issues at stake.[32] Frames shape our understanding of what is going on, why, what (if anything) needs to be done, and who needs to do it. This may involve setting the terms of the argument, for example in relation to existing law or other policy

28 See J.-M. Henckaerts and L. Doswald-Beck, above note 1, Chapter 4; and B. Rappert, above note 17.
29 See the section on 'framing' below.
30 Collin King, Ove Dullum and Grethe Østern, *M85: An Analysis of Reliability*, Norwegian People's Aid, Oslo, 2007.
31 See John Borrie, *Unacceptable Harm*, United Nations, Geneva, 2009.
32 William A. Gamson and André Modigliani, 'Media discourse and public opinion on nuclear power: a constructionist approach', in *American Journal of Sociology*, Vol. 95, No. 1, 1989, pp. 1–37.

commitments; and it may include stipulating which fora are most appropriate. Without the latter, issues might be widely regarded as problems, but not tackled anywhere. Thus, while framing itself requires communication, it is primarily a process of setting the terms for the communication that is to follow.

It is worth noting the different grounds on which civil society and others have raised concerns about particular weapons technologies in the past. There are various subtleties to how concerns have been framed in different contexts. However, some of the grounds for calling for controls on specific weapons could be summarized as follows:

- The weapons, due to the way in which they function, have a tendency to kill or injure the wrong people (e.g., biological, chemical, nuclear weapons, cluster munitions, anti-personnel mines, incendiary weapons).
- The weapons have presented a historical pattern of killing and injuring the wrong people (e.g., anti-personnel mines, cluster munitions).
- The weapons, due to the way in which they function, have a tendency to kill or injure even the intended people in the wrong way (e.g., blinding laser weapons, 'dum-dum' bullets, anti-personnel mines, biological, chemical, and incendiary weapons, cluster munitions in the 1970s).
- The weapons may have wider negative effects on the environment, infrastructure, economic life, etcetera, that last far beyond the period of conflict (e.g., chemical, biological, and nuclear weapons, uranium weapons, landmines and unexploded ordnance).
- The weapons end up in the hands of the wrong people (e.g., in relation to the transfer of 'dual use' technologies and small arms).

In making these arguments, different individuals and organizations may take different orientations to existing law. Some groups tend to urge that, on the basis of one or other of the arguments above, the weapon in question falls foul of existing law by being indiscriminate, causing unnecessary suffering, etcetera. Others might press that, while not straightforwardly disallowed by existing law, one or other of the arguments above provides grounds for new rules to be put in place. Legal, extra-legal, and non-legal arguments run in tandem with assessments about whether new formal rules and restrictions are required and/or whether the delegitimization and stigmatization of weapons within the international community can address identified problems. Such varied orientations are not necessarily mutually incompatible, and within civil society coalitions those with different orientations may still work effectively together.[33]

A key element of civil society responses to new weapon technologies will be to frame the concerns associated with a particular technology. It should be

33 For a discussion on some of the ways in which the Cluster Munition Coalition worked together despite the differing approaches of some of its NGO members, see Thomas Nash, 'Civil society and cluster munitions: building blocks of a global campaign', in M. Kaldor, S. Selchow and H. L. Moore (eds), *Global Civil Society 2012: Ten Years of Critical Reflection*, Palgrave Macmillan, London, 2012, pp. 124–143.

noted that how a weapon is portrayed as a problem can change over time. As is illustrated in the list above, diplomatic proposals in the 1970s to control cluster munitions were framed around concerns regarding unnecessary suffering and superfluous injury (due to the fragmentation effects of the cluster munitions),[34] yet this 'problem' barely featured in the development of an international ban on cluster munitions in 2008.[35] It is not yet clear what framings will predominate with respect to weapon technologies now emerging, but some suggested possibilities are:

- cyber warfare – due to the type of target that may be attacked (e.g., public infrastructure), is likely to harm the wrong people; may cause unforeseeable longer-term harms; and may end up in the hands of the wrong people;
- autonomous weapons – due to the way in which they function (e.g., by sensor/algorithm decisions to attack), will be prone to killing and injuring the wrong people; may lack adequate human accountability; and may offend against an assumption of human control over lethal decisions;
- directed energy weapons – due to the way in which they function (e.g., invisibility of microwaves, unknown longer-term effects, incomprehension of the victims), will cause death and injury in the wrong way, including intended targets.

In all such framings, consideration needs to be given not only to the basic moral problem being attributed to the weapons, but also to the causal link between the technology and the harm. Is the problem that an unacceptable outcome will occur in all circumstances, most circumstances, some circumstances, etcetera? Furthermore, it is possible that new technologies will bring to the fore problem framings that have not been used for weapons previously or that relate back to controls over the methods of warfare rather than weapons as types of technologies. For example, drones have raised concerns about a lack of accountability for attacks with such systems.[36] Both in cyber warfare and the proliferation of drones, the problem might not be framed so much in the permissibility of the weapon technology itself, but in the types of attacks that this technology now facilitates. In any case, the way in which a problem is framed will have a great bearing on the type of solution that follows.

Redefining

'Redefining' means providing an overarching mode of analysis that goes beyond the question of how issues with individual weapon types are framed. Past efforts, spearheaded by international civil society, to shift from traditional national security-indebted arms control approaches to 'human security' or 'humanitarian action'

34 See Eric Prokosch, *The Technology of Killing: A Military and Political History of Anti-Personnel Weapons*, Zed Books, London, 1995, pp. 149–150.
35 See J. Borrie, above note 31.
36 See Philip Alston, 'The CIA and targeted killings beyond borders', in *Harvard National Security Journal*, Vol. 2, 2011, pp. 283–446.

represent instances of redefinition.[37] By linking discussion about the rights and wrongs in the conduct of conflict to these overarching notions of human security and humanitarian action, a goal of the redefinition was to open up novel possibilities for collaboration and paths for intervention.[38] Similarly to 'framing' discussed above, the work of redefining modes of analysis is about setting the terms of technical, political, or public arguments that will subsequently be worked through.

Redefinitions might be more or less explicit or acknowledged. By shifting from a negotiation process structured around establishing what should be restricted to instead demanding argument for what should be allowed, Rappert and Moyes argued that the Oslo Process leading to the Convention on Cluster Munitions shared important dimensions with 'precautionary' approaches to environmental risk.[39] Borrie has noted that 'shifting the burden of proof' was a key (though not often remarked upon) element in the development of the case against cluster munitions.[40] Yet, while some in this process recognized the significance of this shift, many others may not have done.[41] As a result, the precautionary precedents set by the Oslo Process may, or may not, inform a wider redefinition in how future negotiation processes are structured.

As an approach that is wider than armed conflict, conceptualizing violence as a health problem is an approach that can both complement and challenge legal and security-related agendas. Shared starting points among health approaches include conceptualizing violence as a substantial and preventable cause of physical and psychological harm.[42] Public health approaches have been advanced in relation to armed conflict in general,[43] and small arms in particular.[44] Bound up with such redefinitions has been the expansion of what kinds of expertise are required; specifically, an extension of expertise beyond that associated with military operations and legal rules.

Aligned with health definitions, the argument has been advanced that some classes of weapons need to be scrutinized as if they were drugs. This is most evident today in relation to biochemical agents alternatively known as

37 J. Borrie and V. Randin (eds), *Disarmament as Humanitarian Action*, UNIDIR, Geneva, 2006, pp. 23–50.

38 Such an approach is currently gaining greater prominence in discussions on nuclear weapons. In May 2012, sixteen states led by Switzerland delivered a statement on the humanitarian dimension of nuclear disarmament during a meeting of the Nuclear Non-Proliferation Treaty. See Rebecca Johnson, 'Non-Proliferation Treaty: the ground is shifting', Open Democracy, 4 May 2012, available at: http://www.opendemocracy.net/5050/rebecca-johnson/non-proliferation-treaty-ground-is-shifting (last visited 10 May 2012).

39 Brian Rappert and Richard Moyes, 'The prohibition of cluster munitions: setting international precedents for defining inhumanity', in *Non-proliferation Review*, Vol. 16, No. 2, 2009, pp. 237–256.

40 J. Borrie, above note 31.

41 *Ibid*., and Brian Rappert, Richard Moyes and A. N. Other, 'Statecrafting ignorance: strategies for managing burdens, secrecy, and conflict', in S. Maret (ed.), *Government Secrecy (Research in Social Problems and Public Policy, Volume 19)*, Emerald, London, 2011, pp. 301–324.

42 World Health Organization, *Preventing Violence: A Guide to Implementing the Recommendations of the World Report on Violence and Health*, WHO, Geneva, 2004.

43 Maria Valenti, Christin M. Ormhaug, Robert E. Mtonga and John E. Loretz, 'Armed violence: a health problem, a public health approach', in *Journal of Public Health Policy*, Vol. 28, No. 4, 2007, pp. 389–400.

44 Small Arms Survey, *SmallArms Survey 2008*, Oxford University Press, Oxford, 2008, Chapter 7.

'incapacitating', 'non-lethal', and 'less lethal' weapons. The use of a fentanyl derivative during the Moscow theatre siege in October 2002 (with tragic results) is the most high-profile example of such a weapon capability, a capability that may yet be adopted more widely by other governments. In the light of such developments, many have questioned the legality of such options as well as the adequacy of the procedures meant to validate their safety.[45]

The contention that the uncertain or unpredictable effects of chemical agents require a wider appraisal of their acceptability goes back some time. In light of widespread use of CS smoke ('tear gas') grenades in Northern Ireland in the late 1960s, the UK government-appointed Himsworth Committee concluded, among other things, that in the future such chemical agents should be regarded as being more akin to medical drugs than weapons in relation to their operational approval.[46] While the specific meaning of this recommendation is open to question, arguably any such process would need to consist at least of the pre-deployment testing for possible concerns in a manner open to scrutiny and the post-deployment monitoring of operational use. Making public the evidential basis for decisions. as well as the criteria for assessment, would be vital in ensuring the robustness of decisions and the adequacy of attempts to address uncertainties. As with the monitoring of adverse reactions to drugs, rigorous systems for the post-marketing surveillance of weapons' effects would also be vital in ensuring that outcomes match expectations.

Thus, treating weapons as akin to medical drugs for the purpose of their assessment and control is one way civil society could redefine current approaches to these technologies. The next section illustrates the gulf between such an aspiration and state practice, and thereby the sweeping changes possible through such a redefinition.

Communicating and representing

A fifth role for civil society is in the ongoing communication and representation of this information, analysis, and problem framings to different audiences. The work of communication is seen in NGO publications, placing of media stories, interventions in meetings, mobilization of parliamentarians, and direct lobbying of diplomats and government officials. Such communications may be setting the agenda, framing arguments, pushing for decisions, supporting negotiations, or monitoring instruments already in place. However, underpinning this representational role there is a wider question about how affected populations have their voices heard in discussions regarding the acceptability or appropriateness of certain weapons.

Weapons of armed conflict are often developed and brought into service with assumption that the population amongst whom they may be used will be foreign rather than domestic. As a result, the links of accountability between those

45 British Medical Association, *The Use of Drugs as Weapons*, BMA, London, 2007.
46 Himsworth Committee, *Report of the enquiry into the medical and toxicological aspects of CS*. Part 2, Cmnd 4775, HMSO, London, 1971.

introducing the technology and those likely to experience negative effects are very limited. By representing the experiences of that population, civil society organizations can work to reduce this deficit in accountability. The development of global civil society coalitions, where many NGOs in different countries share resources and coordinate their research and advocacy work under a common banner, can help to increase the space for often-marginalized perspectives to be heard.[47] However, capacity in that area is arguably significantly short of what might be required to sustain a systematic scrutiny of weapon effects and implications across the range of relevant theatres and technologies.

A representational role also brings with it challenges. Civil society often presents itself as 'speaking on behalf of' populations, but the basis for such a mandate is often unclear. Cluster munition survivors, as activists against cluster munitions, had a strong and active role in the process of banning these weapons, but in any such process there are dangers that 'victims' are used as representational figureheads and are without the authority to manage representation directly. Making assertions about what affected communities need and about where any particular issue stands amongst those communities' priorities is fraught with difficulties for those in civil society. Civil society organizations often face pressure to synthesize diverse experience into a sense of the problem that can fit into the political debate at hand. However, this might downplay or exclude some of the experiences of those in affected communities. For instance, in the case of cluster munitions much of the focus was on civilian populations. This differs significantly from the attention given to these weapons in the 1970s when effects on military personnel were the centre of attention. Despite these concerns about who is represented, such a representational role will likely remain a key one for civil society as state willingness to bring affected populations directly into discussions regarding the acceptability of certain weapons remains very limited.

Strengthening the review of new weapons, means, and methods of warfare

The sections above have considered some of the key roles that civil society currently undertakes in the development of standards regarding weapon technologies. It can be seen that civil society has a major role in such processes, yet this role is almost wholly informal (i.e., it is not mandated by any particular instrument). The capacity of civil society in relation to this work is also limited. In many respects, civil society can be seen as informally taking on broad roles that the state might be expected to carry out; that is, processes to assess the acceptability of technologies that are not currently being undertaken effectively by states and other actors who are primarily responsible for the development and deployment of such technologies. In light of

47 For a discussion on global civil society coalitions, see Richard Moyes and Thomas Nash, *Global Coalitions: An Introduction to Working in International Civil Society Partnerships*, Action on Armed Violence, London, 2011, available at: www.globalcoalitions.org (last visited 20 May 2012).

the above sections, we briefly examine below the current status of formal processes used by states for assessing weapons, which focus principally on concerns regarding such weapons' legality under existing obligations.

International law provides a framework for applying legal standards in the development of new technologies of warfare: Article 36 of Additional Protocol I to the Geneva Conventions of 1949. Article 36 requires that state parties assess new weapons, means, or methods of warfare for compliance with Additional Protocol I and international law more broadly.[48] As the ICRC has said:

> The aim of Article 36 is to prevent the use of weapons that would violate international law in all circumstances and to impose restrictions on the use of weapons that would violate international law in some circumstances, by determining their lawfulness before they are developed, acquired or otherwise incorporated into a State's arsenal.[49]

The importance of the Article 36 obligation should not be understated: states are bound to undertake legal reviews of new technologies of warfare and they must consider whether the use of these new technologies would be contrary to international law in some or all circumstances. A failure to do so renders a state internationally responsible for a breach of its obligations vis-à-vis the other parties to Additional Protocol I.[50] For those states that are not party to Additional Protocol I, review should arguably be undertaken as a corollary to other international obligations, or as a matter of best practice.[51] The United States of America is one notable example of a state that is not party to Additional Protocol I, but which nonetheless carries out legal reviews of new weapons. In an effort to strengthen international implementation of this rule States Parties to the UN Convention on Certain Conventional Weapons (CCW) have also recognized the importance of weapons reviews. For example, the Final Declaration of the 4th CCW Review Conference highlights the determination of States Parties 'to urge States which do not already do so to conduct reviews to determine whether any new weapon, means or methods of warfare would be prohibited under international humanitarian law or other rules of international law applicable to them'.[52]

The ICRC has made efforts to promote compliance with Article 36. Successive international conferences of the Red Cross and Red Crescent have urged

48 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

49 ICRC, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*, Geneva, 2006, p. 4.

50 Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Martinus Nijhoff Publishers, Geneva, 1987, p. 423.

51 ICRC, *Guide*, above note 49, p. 4; Isabelle Daoust, Robin Coupland and Rikke Ishoey 'New wars, new weapons? The obligation of states to assess the legality of means and methods of warfare', in *International Review of the Red Cross*, Vol. 84, No. 846, June 2002, p. 348; Darren Stewart, 'New technology and the law of armed conflict', in Raul A. 'Pete' Pedrozo and Daria P. Wollschlaeger (eds), *International Law and the Changing Character of War*, Naval War College, Newport, Rhode Island, 2011, p. 283.

52 UN Convention on Certain Conventional Weapons, UN Doc. CCW/CONF.IV/4/Add.1, p. 4.

states to engage in legal reviews of weapons. Notably, the 2003 conference adopted a Declaration and Agenda for Humanitarian Action, which included as a goal:[53]

> In light of the rapid development of weapons technology and in order to protect civilians from the indiscriminate effects of weapons and combatants from unnecessary suffering and prohibited weapons, all new weapons, means and methods of warfare should be subject to rigorous and multidisciplinary review.

To this end, the ICRC has provided significant guidance on weapons reviews in the form of its 2006 publication *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare*.[54] The *Guide* outlines the types of weapons subject to review, the rules to be applied to new weapons, means, and methods of warfare, and the data that reviewers should consider (including health- and environment-related considerations). Drawing on existing practice, it makes suggestions as to the legal status and location of the review body within government, and its structure and composition. It also describes how the review process may operate and provides examples of possible rules and structures for decision-making.

The challenges of reviews

Before offering an evaluation of the implementation of Article 36 – and thereby illustrating the scope for civil society engagement – it is worth noting some of the general difficulties associated with the type of reviews that might be envisioned based on an analysis of such processes in relation to technologies more broadly. Collingridge[55] identified a fundamental dilemma in trying to manage technology. Controls are relatively easy to introduce in the early stages of development, yet at such an early stage they often prove difficult to justify because negative effects have not materialized. However, when the need for controls is apparent because of negative effects they are often more expensive and troublesome to put in place. The way technologies become entrenched within organization practice, the investment costs already committed, the formation of beliefs and career structures, etcetera, can all work against the adoption of control measures.

Collingridge's key recommendation is to maintain flexibility in the adoption of a technology. The customary response to the 'dilemma of control' is to focus on finding better ways of forecasting technology's effects. This approach has limitations given the fallibilities of analysis. In the case of weaponry, the fallibility of analysis is particularly acute because of the scope for uncertainty and disagreement about costs and benefits (including how such costs and benefits are characterized) and the substantial and irreversible nature of the harms that might be inflicted. In

53 See 28th International Conference of the International Red Cross and Red Crescent Movement, Geneva, Switzerland, 2–6 December 2003, final goal 2.5. *Resolution 1: Adoption of the Declaration and Agenda for Humanitarian Action.* Review of new weapons was also urged in the Final Document of the Fourth Review Conference of the Convention on Certain Conventional Weapons, November 2011, CCW/CONF.IV/4/Add.1, para. 16.

54 ICRC, *Guide*, above note 49.

55 David Collingridge, *The Social Control of Technology*, St. Martin's, New York, 1980.

these circumstances, it is vital that processes are established for learning from experience. This underscores the need for openness to scrutiny, involvement of those with expertise and relevant backgrounds, ongoing review of operational use, and the open sharing of experiences.

The challenges of existing practice

However, current implementation of Article 36 seems to fall far short of the type of regime suggested in the paragraph above. While progressive in its intent, Article 36 is reactionary in its terms, which do not prescribe any particular mode of compliance. Instead it is left to states to determine their own processes without international oversight. Consequently, it is difficult to gain a complete picture of whether, or to what extent, states are abiding by the obligation to review. In the context of national defence and security interests there is a dearth of publicly available information on weapons review programmes and their outputs. As Cassese noted shortly after the adoption of Additional Protocol I, Article 36 does not require states to make public their weapons reviews and, consequently, 'other contracting States have no possibility of verifying whether the obligation laid down [in Article 36] is complied with'.[56] Such secrecy presents particular challenges for civil society organizations that seek to enhance state accountability and promote transparency.

Further, Article 36 is quite evidently not self-executing. Despite the scope afforded to national authorities in determining the mode of compliance with its terms, more than three decades after Protocol I's adoption the number of states known to have formal review processes remains very small. While a limited number of states appear to be actively abiding by the terms of Article 36, it is clear that a much larger number of states are not undertaking weapons reviews.[57] It also appears that some states rely on the review processes of larger military powers when they acquire or develop new weapons, failing to abide by their independent obligation to review.[58]

While states are entitled to calibrate their review processes differently, many interpret the Article 36 obligation very narrowly. This tendency can manifest

56 Antonio Cassese, 'Means of warfare: the traditional and the new law', in A. Cassese (ed.), *The New Humanitarian Law of Armed Conflict (Vol. 1)*, Editoriale scientifica, Naples, 1979, p. 179.

57 Seven states appear to have formal review processes, the details of which are publicly available: Australia, Belgium, the Netherlands, Norway, Sweden, the United Kingdom, and the United States of America. A further three states, Denmark, France, and Germany, are thought to have formal review processes, but information about these processes does not appear to be publicly available. There are another thirteen states that have indicated that they may have informal or formal review processes, but have not made sufficient information available to determine whether this is the case (formal: Canada, Czech Republic, New Zealand, Russian Federation, Switzerland; informal: Austria, Brazil, Croatia, Finland, Mexico, Poland, Portugal, and South Africa). See, ICRC, *Reaffirming and Implementing International Humanitarian Law* (Follow-up to Resolution 3 of the 30th International Conference), October 2011 : 'Despite pledges made by some States at the 2007 International Conference, the ICRC is not aware of the establishment of any procedures to review the legality of new weapons in a State that did not already have such a mechanism.'

58 ICRC, *Follow-up to the 28th International Conference: Report prepared for the 30th International Conference of the Red Cross and Red Crescent*, ICRC, Geneva, 2007, p. 25.

itself in at least four different ways: first, through a primary focus on ensuring technologies in development will not fall into existing categories of explicitly banned weapons, neglecting, or downplaying the applicability of a broader range of general rules that are more difficult to interpret; second, the phrase 'weapons, means or methods of warfare' may be interpreted to refer only to physical weapons and their normal or intended use, with the meaning of 'means or methods of warfare' poorly understood and not extending to the ways in which certain weapons are used;[59] third, while some states take on board the multidisciplinary approach urged by the ICRC, involving experts from a variety of disciplines in the evaluation process, others leave the determination to military lawyers or 'experts' who need not draw on outside inputs despite their obvious relevance to the question of legality;[60] and, finally, most states fail to review existing technologies on an ongoing basis, in light of actual battlefield use and effects. In addition, this analysis is generally done in secret with little or no public information being produced to facilitate learning lessons from the past or from other contexts. As a result, even where they are followed, such processes will tend to produce narrow legal interpretations and thus are unlikely to provide a substantial barrier to the uptake of new weapon systems that present unknown risks. In some cases, states have asserted reservations under Additional Protocol I that seek to exempt whole categories of weapons from falling under those rules. For example, the UK government's reservation to Additional Protocol I states, inter alia, that 'the rules so introduced do not have any effect on and do not regulate or prohibit the use of nuclear weapons'.[61]

Engendering a culture of review

Many of the known review processes appear to be ill-suited to assessing certain new technologies of warfare for compliance with international law. First, the acquisition or development of some new technologies will simply not be subject to review at all: either that technology will fall outside the narrow definition generally accorded to 'weapons, means or methods of warfare' (as may be the case with many cyber capabilities[62]) or its development will occur outside normal military processes and

59 The Commentary to Article 36 endorses a conservative approach regarding which uses of weapon should be considered, confining the analysis to 'normal or expected use'. Fry takes the view that the Commentary (and, by extension, the *Guide*, which endorses this aspect of the Commentary) takes an unnecessarily narrow view on this point. James D. Fry, 'Contextualized legal reviews for the methods and means of warfare: cave combat and international humanitarian law', in *Columbia Journal of Transnational Law*, Vol. 44, 2006, p. 453: 'The phrase "in some or all circumstances" [in Article 36] does not unreasonably oblige states to foresee absolutely all uses of a weapon or method of warfare. However, it does indicate that the commentators are far too passive in interpreting Article 36. Indeed, "in some or all circumstances" suggests that these legal reviews must consider anticipated uses of weapons beyond those that are considered "normal." . . . Moreover, . . . significant changes in anticipated use or use itself calls for repeated review of legality to ensure continued compliance with international law, even after initial deployment of a weapon or method'.

60 ICRC, *Follow-up to the 28th International Conference*, above note 58, p. 25.

61 UK Government, The Geneva Conventional Act (First Protocol) Order 1998, Schedule (a), available at: http://www.legislation.gov.uk/uksi/1998/1754/schedule (last visited 20 May 2012).

62 The US Air Force, however, explicitly includes cyber capabilities within the scope of review: *Legal Reviews of Weapons and Cyber Capabilities*, Air Force Instruction 51-402, 27 July 2011.

so fail to come to the attention of the bureaucratic apparatus charged with undertaking review. Second, if review does occur, there may be insufficient expertise or capacity within the review body, or those it seeks input from, to adequately understand the operation and effects of the technology. Third, the frame for assessing legality often incorporates the narrow interpretations described above, where only 'normal' or expected uses of the technology are considered (with little by way of a boundary established to prevent use outside of such parameters) and no reassessment is made on the basis of actual use and actual effects post-review. Finally, even if a broad approach is taken, existing international law, with its open terms and focus on 'balances', may be reasonably interpreted as not addressing the technology or allowing the technology, despite concerns about its humanitarian or environmental impact. These inadequacies should be cause for significant concern: democratic states have a duty to justify the deployment of new technologies that may inappropriately kill, injure, or cause wider harms in both moral and legal terms – even if some form of harm is part of the designed purpose of the technology.

The military application of nanotechnology provides a concrete example of the inadequacies of the current framework. Nasu and Faunce observe that:

> the practical value [of principles of international humanitarian law] in regulating nano-weapons is significantly hampered by indeterminacy, diverse interpretations, and scientific uncertainty that become obvious when the principles are applied to a specific new weapon.[63]

As they note, '[t]echnological advancement all too often entails adverse effects on the environment or human health that may not immediately be so obvious after its full import into battlefields is experienced'.[64] Further, where significant investment and time have been devoted to a new technology, the pressure on military lawyers to defend its legality may be very great, even if unstated; for example, in the absence of clear evidence of adverse long-term effects, the confidently claimed military advantages of the technology may allow reviewers to strike the balance between military considerations and possible harm in favour of legality.[65] In such a case the standards of proof required of the different elements being balanced may be quite different.

While the creation of an international body charged with scrutinizing new technologies is politically implausible right now, some mechanism for strengthening international capacity and coordination is required.[66] The role of civil society aside, formalized coordination between states in shaping standards around new technologies could be a significant part of the solution. The responsibility for

63 Hitoshi Nasu and Thomas A. Faunce, 'Nanotechnology and the international law of weaponry: towards international regulation of nano-weapons', in *Journal of Law, Information and Technology*, Vol. 20, 2010, p. 53.
64 *Ibid.*, p. 47.
65 *Ibid.*, p. 48.
66 See Marie Jacobsson, 'Modern weaponry and warfare: the application of Article 36 of Additional Protocol I by governments', in Anthony M. Helm (ed.), *The Law of War in the 21st Century, Weaponry and the Use of Force*, Naval War College, Newport R.I., 2006, p. 184.

carefully considering each new technology and its relationship to legality and broader considerations of humanity should be a shared one, including during the conceptualization, design, and manufacture of weapons. However, it is not clear from current practice that states are undertaking their responsibilities in a way that adequately assesses the humanitarian and moral problems that weapons technologies can pose. Without greater transparency and sharing of information it is hard to see that the national-level processes currently in place can provide the basis for more progressive efforts to set standards regarding weapons. There are few if any examples of weapons that have been found to be problematic through a national review mechanism and where the state has then gone on to promote a new international standard with respect to the particular technology. Similarly, there are few if any examples of states revisiting their reviews of weapon legality in the wake of evidence that existing weapons are causing unacceptable humanitarian or environmental harm.

Conclusion

The picture outlined in this article is of civil society undertaking a range of broad informal roles with respect to setting new moral and legal standards regarding weapons, contrasted with formal national-level mechanisms that are narrowly defined and opaque. Civil society's roles are 'informal' in so far as they are not generally mandated by any official body. They tend to be ad hoc and gradual and develop momentum on particular issues due to the convergence of a wide range of factors relating to the problems and opportunities presented. However, across all of these functions civil society is working with limitations on available resources, with the funding that goes into the development of new technologies far outstripping the money that goes into documenting harm, analysing that data, and mobilizing political consideration of the issues. A particular challenge for civil society with respect to weapons will be the prioritization of resources for specific issues in a context where a range of new technologies raise moral or humanitarian concerns for the future. Bound up with this is the risk that attention to such new technologies, which may spark public and media engagement, may draw focus and resources away from existing weapon technologies that are already creating patterns of distinct and severe humanitarian harm. In such a context, giving critical attention to the mechanisms by which new weapon technologies are assessed may provide an efficient entry point for critiquing a range of emerging technologies.

While critical engagement in weapon review processes may be developed at a national level this would be substantially augmented by the presence of international fora where weapons can be discussed in some detail. At present it is only the UN Convention on CCW that can provide space for consideration of various weapon technologies under its existing mandate, yet this mechanism has spent much of the last decade focused on explosive remnants of war, anti-vehicle mines, and cluster munitions (despite cluster munitions already being subject to international legal prohibition). While the UN Convention on CCW provides

relatively good access to civil society to present data and engage in debate, and has in the past given attention to areas of new technology (for example, blinding laser weapons), the consensus-based process for establishing the agenda might limit consideration of weapons where certain states are strongly opposed to greater transparency about those weapons. The same consensus-based approach is also likely to severely limit the extent to which any new prohibitions or restrictions can be adopted within that framework. In order to strengthen standard-setting in such a context in the short-term, civil society is likely to have to focus on framing concerns around certain weapons in the public discourse in the hope that such a process will eventually precipitate development of a forum where formalized discussions can be undertaken.

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

COMMENTS AND OPINIONS

The evitability of autonomous robot warfare*

Noel E. Sharkey**

Noel E. Sharkey is Professor of Artificial Intelligence and Robotics and Professor of Public Engagement in the Department of Computer Science at the University of Sheffield, UK, and currently holds a Leverhulme Research Fellowship on an ethical and technical assessment of battlefield robots.

Abstract

This is a call for the prohibition of autonomous lethal targeting by free-ranging robots. This article will first point out the three main international humanitarian law (IHL)/ ethical issues with armed autonomous robots and then move on to discuss a major stumbling block to their evitability: misunderstandings about the limitations of robotic systems and artificial intelligence. This is partly due to a mythical narrative from science fiction and the media, but the real danger is in the language being used by military researchers and others to describe robots and what they can do. The article will look at some anthropomorphic ways that robots have been discussed by the military and then go on to provide a robotics case study in which the language used obfuscates the IHL issues. Finally, the article will look at problems with some of the current legal instruments and suggest a way forward to prohibition.

Keywords: autonomous robot warfare, armed autonomous robots, lethal autonomy, artificial intelligence, international humanitarian law.

* The title is an allusion to a short story by Isaac Asimov, 'The evitable conflict', where 'evitable' means capable of being avoided. Evitability means avoidability.

** Thanks for comments on earlier drafts go to Colin Allen, Juergen Altmann, Niall Griffith, Mark Gubrud, Patrick Lin, George Lucas, Illah Nourbakhsh, Amanda Sharkey, Wendell Wallach, Alan Winfield, and to editor-in-chief Vincent Bernard and the team of the *International Review of the Red Cross*, as well as others who prefer to remain unnamed.

doi:10.1017/S1816383112000732

We could be moving into the final stages of the industrialization of warfare towards a factory of death and clean-killing where hi-tech countries fight wars without risk to their own forces. We have already seen the exponential rise of the use of drones in the conflicts in Iraq and Afghanistan and by the US Central Intelligence Agency for targeted killings and signature strikes in countries outside the war zones: Pakistan, Yemen, Somalia, and the Philippines. Now more than fifty states have acquired or are developing military robotics technology.[1]

All of the armed robots currently in use have a person in the loop to control their flight and to apply lethal force. But that is set to change soon. Over the last decade the roadmaps and plans of all US forces have made clear the desire and intention to develop and use autonomous battlefield robots. Fulfilment of these plans to take the human out of the control loop is well underway for aerial, ground, and underwater vehicles. And the US is not the only country with autonomous robots in their sights. China, Russia, Israel, and the UK are following suit. The end goal is a network of land, sea, and aerial robots that will operate together autonomously to locate their targets and destroy them without human intervention.[2]

IHL and ethical issues with lethal autonomous robots

A major IHL issue is that autonomous armed robot systems cannot discriminate between combatants and non-combatants or other immune actors such as service workers, retirees, and combatants that are wounded, have surrendered, or are mentally ill in a way that would satisfy the principle of distinction. There are systems that have a weak form of discrimination. For example, the Israeli Harpy is a loitering munition that detects radar signals. When it finds one, it looks at its database to find out if it is friendly and if not, it dive bombs the radar. This type of discrimination is different from the requirements of the principle of distinction because, for example, the Harpy cannot tell if the radar is on an anti-aircraft station or on the roof of a school.

Robots lack three of the main components required to ensure compliance with the principle of distinction. First, they do not have adequate sensory or vision processing systems for separating combatants from civilians, particularly in insurgent warfare, or for recognizing wounded or surrendering combatants. All that is available to robots are sensors such as cameras, infrared sensors, sonars, lasers, temperature sensors, and ladars etc. These may be able to tell us that something is a human, but they could not tell us much else. There are systems in the labs that can recognize still faces and they could eventually be deployed for individual targeting in limited circumstance. But how useful could they be with

1 Noel Sharkey, 'The automation and proliferation of military drones and the protection of civilians', in *Journal of Law, Innovation and Technology*, Vol. 3, No. 2, 2001, pp. 229–240.

2 Noel Sharkey, 'Cassandra or the false prophet of doom: AI robots and war', in *IEEE Intelligent Systems*, Vol. 23, No. 4, 2008, pp. 14–17.

moving targets in the fog of war or from the air? British teenagers beat the surveillance cameras simply by wearing hooded jackets.

Second, a computer can compute any given procedure that can be written down in a programming language. This is rather like writing a knitting pattern or recipe. We also need to be able to specify every element in sufficient detail for a computer to be able to operate on it. The problem for the principle of distinction is that we do not have an adequate definition of a civilian that we can translate into computer code. The laws of war does not provide a definition that could give a machine with the necessary information. The 1949 Geneva Convention requires the use of common sense, while the 1977 Protocol I defines a civilian in the negative sense as someone who is not a combatant.[3]

Third, even if machines had adequate sensing mechanisms to detect the difference between civilians and uniform-wearing military, they would still be missing battlefield awareness or common sense reasoning to assist in discrimination decisions. We may move towards having some limited sensory and visual discrimination in certain narrowly constrained circumstances within the next fifty years. However, I suspect that human-level discrimination with adequate common sense reasoning and battlefield awareness may be computationally intractable.[4] At this point we cannot rely on machines ever having the independent facility to operate on the principle of distinction as well as human soldiers can.[5] There is no evidence or research results to suggest otherwise.

A second IHL issue is that robots do not have the situational awareness or agency to make proportionality decisions. One robotics expert has argued that robots could calculate proportionality better than humans.[6] However, this concerns the *easy proportionality problem*: minimizing collateral damage by choosing the most appropriate weapon or munition and directing it appropriately. There is already software called bugsplat used by the US military for this purpose. The problem is that it can only ease collateral impact. For example, if munitions were used near a local school where there were 200 children, the appropriate software may mean that only fifty children were killed rather than all had a different bomb been used.

The *hard proportionality problem* is making the decision about whether to apply lethal or kinetic force in a particular context in the first place. What is the balance between loss of civilian lives and expected military advantage? Will a particular kinetic strike benefit the military objectives or hinder them because it upsets the local population? The list of questions is endless. The decision about what is proportional to direct military advantage is a human qualitative and subjective

3 Article 50(1) of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, 8 June 1977 (hereinafter Additional Protocol I)

4 As a scientist I cannot exclude the notion that some black swan event could change my scepticism, but at present we certainly cannot rely on this as a credible option in discussions of lethal force and the protection of innocents.

5 See Noel E. Sharkey, 'Grounds for Discrimination: Autonomous Robot Weapons', in *RUSI Defence Systems*, Vol. 11, No. 2, 2008, pp. 86–89.

6 Ronald C. Arkin, *Governing Lethal Behavior in Autonomous Systems*, CRC Press Taylor & Francis Group, Boca Raton F.L., 2009, pp. 47–48.

decision. It is imperative that such decisions are made by responsible, accountable human commanders who can weigh the options based on experience and situational awareness. When a machine goes wrong it can go really wrong in a way that no human ever would.

I turn to the well-known expression that much of war is art and not science. Or as Col. David M. Sullivan, an Air Force pilot with extensive experience with both traditional and drone airstrikes from Kosovo to Afghanistan, told *Discover* magazine: 'If I were going to speak to the robotics and artificial intelligence people, I would ask, "How will they build software to scratch that gut instinct or sixth sense?" Combat is not black-and-white'.[7]

Arguing against a ban on lethal autonomous robot weapons, Anderson and Waxman state that some leading roboticists have been working on creating algorithms to capture the two fundamental principles of distinction and proportionality. But they cite only one roboticist: 'One of the most ambitious of these efforts is by roboticist Ronald C. Arkin, who describes his work on both distinction and proportionality in his "Governing Lethal Behavior".'[8] But this is mistaken because while this roboticist discusses both principles, he is not conducting research on either of them. He only suggests that they will be solvable by machines one day.

The work Anderson and Waxman cite is, in fact, merely a suggestion for a computer software system for the ethical governance of robot 'behaviour'.[9] This is what is known as a 'back-end system'. Its operation relies entirely on information from systems yet 'to be developed' by others sometime in the future. It has no direct access to the real world through sensors or a vision system and it has no means to discriminate between combatant and non-combatant, between a baby and a wounded soldier, or a granny in a wheelchair and a tank. It has no inference engine and certainly cannot negotiate the types of common sense reasoning and battlefield awareness necessary for discrimination or proportionality decisions. There is neither a method for interpreting how the precepts of the laws of war apply in particular contexts nor is there any method for resolving the ambiguities of conflicting laws in novel situations.

A third issue is accountability.[10] A robot does not have agency, moral or otherwise, and consequently cannot be held accountable for its actions. Moreover, if autonomous robots were used in limited circumstances in the belief that they could operate with discrimination, it would be difficult to decide exactly who was accountable for mishaps. Some would say that the commander who gave the order to send the robot on a mission would be responsible (last point of contact). But that would not be fair since it could be the fault of the person who programmed the

7 Mark Anderson, 'How Does a Terminator Know When to Not Terminate', in *Discover Magazine*, May 2010, p. 40.

8 Kenneth Anderson and Matthew Waxman, 'Law and Ethics of Robot Soldiers', in *Policy Review*, in press 2012.

9 See R. C. Arkin, above note 6.

10 Robert Sparrow, 'Building a Better WarBot: Ethical Issues in the Design of Unmanned Systems for Military Applications', in *Science and Engineering Ethics*, Vol. 15, No. 2, 2009, pp.169–187.

mission, the manufacturer who made the robot, or the senior staff or policymakers who decided to deploy it. Or it could be claimed that the device was tampered with or damaged. Anderson and Waxman dismiss the accountability objection out of hand:

> Post hoc judicial accountability in war is just one of many mechanisms for promoting and enforcing compliance with the laws of war, and devotion to individual criminal liability as the presumptive mechanism of accountability risks blocking development of machine systems that would, if successful, reduce actual harms to civilians on or near the battlefield.[11]

But I disagree. Using a weapon without a clear chain of accountability is not a moral option. Without accountability to enforce compliance many more civilian lives could be endangered.

On the basis of these three issues, I will argue here that the morally correct course of action is to ban autonomous lethal targeting by robots. Before looking at problems with the legal instruments, I will first examine a major stumbling block to a prohibition on the development of armed autonomous robots. A notion proposed by the proponents of lethal autonomous robots is that there are technological 'fixes' that will make them behave more ethically and more humanely than soldiers on the battlefield. I will argue here that this has more to do with descriptive language being used to describe robots rather than what robots can actually do.

Anthropomorphism and mythical artificial intelligence

The common conception of artificial intelligence (AI) and robotics has been distorted by the cultural myth of AI engendered partly by science fiction, by media reporting, and by robotics experts sucked into the myths or seeking public recognition. Robots can be depicted as sentient machines that can think and act in ways superior to humans and that can feel emotions and desires. This plays upon our natural tendency to attribute human or animal properties and mental states (anthropomorphism or zoomorphism) to inanimate objects that move in animal-like ways.[12] We are all susceptible to it and it is what has made puppets so appealing to humans since ancient times.

The myth of AI makes it acceptable, and even customary, to describe robots with an anthropomorphic narrative. Journalists are caught up in it and know that their readers love it. But we cannot just blame the media. It is a compelling narrative and even some roboticists inadvertently feed into the myth. Like other cultural myths, it can be harmless in casual conversations in the lab. But it is a perilous road to follow in legal and political discussions about enabling machines to apply lethal force.

11 See K. Anderson and M. Waxman, above note 8.

12 Amanda Sharkey and Noel Sharkey, 'Artificial Intelligence and Natural Magic', in *Artificial Intelligence Review*, Vol. 25, No. 1–2, 2006, pp. 9–19.

Even with remote-controlled robots, anthropomorphism catches the military. The *Washington Post* reported that soldiers on the battlefield using bomb disposal robots often treat them as fellow warriors and are sometimes prepared to risk their own lives to save them. They even take them fishing during leisure time and get them to hold a fishing rod in their gripper.[13] In the mid-1990s, roboticist Mark Tilden ran a test of his 'Bagman' multipede mine-clearing robot at the Yuma Arizona Missile testing range. Each time that the robot detected a mine, it stamped on it and one leg was blown off. A US colonel watching the legs being blown off one by one finally called a halt to the test because he felt that it was inhumane.[14]

The impact of anthropomorphism can go all the way to the top. Gordon Johnson, former head of the Joint Forces Command at the Pentagon, told the *New York Times* that robots 'don't get hungry. They're not afraid. They don't forget their orders. They don't care if the guy next to them has just been shot.'[15] All of this can also be said of a landmine and my washing machine. Yet if Johnson had said it about these devices, it would have sounded ridiculous. Without being directly anthropomorphic, Johnson is leaking it.

Similarly, Marchant et al. say of robots that 'they can be designed without emotions that cloud their judgment or result in anger and frustration with ongoing battlefield events'.[16] This leaks anthropomorphism because it implies that without special design the robots would have emotions to cloud their judgements. Clearly this is wrong. The myth of robot soldiers even spreads into the law community with titles like 'Law and Ethics of Robot Soldiers'.[17]

A case study of wishful mnemonics

In his influential paper, 'Artificial intelligence meets natural stupidity',[18] Drew McDermott, a Professor of AI at Yale University, expressed concern that the discipline of AI could ultimately be discredited by researchers using natural language mnemonics, such as 'UNDERSTAND', to describe aspects of their programs. Such terms describe a researcher's aspirations rather than what the programs actually do. McDermott called such aspirational terms 'Wishful Mnemonics' and suggested that, in using them, the researcher 'may mislead a lot of people, most prominently himself', that is, the researcher may misattribute

13 Joel Garreau, 'Bots on the Ground', in *Washington Post*, 6 May 2007, available at: http://www.washingtonpost.com/wp-dyn/content/article/2007/05/05/AR2007050501009.html (last visited January 2012).

14 Mark Tilden, personal communication and briefly reported in *ibid.*

15 Tim Weiner, 'New model arm soldier rolls closer to battle', in *New York Times*, 16 February 2005, available at: http://www.nytimes.com/2005/02/16/technology/16robots.html (last visited January 2012).

16 Gary E. Marchant, Braden Allenby, Ronald Arkin, Edward T. Barrett, Jason Borenstein, Lyn M. Gaudet, Orde Kittrie, Patrick Lin, George R. Lucas, Richard O'Meara, Jared Silberman, 'International governance of autonomous military robots', in *The Columbia Science and Technology Law Review*, Vol. 12, 2011, pp. 272–315.

17 See K. Anderson and M. Waxman, above note 8.

18 Drew McDermott, 'Artificial Intelligence Meets Natural Stupidity', in J. Haugland (ed.), *Mind Design*, MIT Press, Cambridge, 1981, pp. 143–160.

understanding to the program. McDermott suggests, instead, using names such as 'G0034' and seeing if others are convinced that the program implements 'understanding'.

Ronald Arkin's work on developing a robot with an artificial conscience provides us with a strong case study to explore what happens when wishful mnemonics and a particular anthropomorphic perception of robots and emotion are applied. He states: 'I am convinced that they [autonomous battlefield robots] can perform more ethically than human soldiers are capable of.'[19] Notice that he does not say that humans could *use* robots in a more ethical manner. Instead, he directs us into the mythical trope that the robots themselves will perform more ethically. This can lead to the mistaken conclusion that robots are capable of moral reasoning in warfare in the same way as humans. Once this premise is in place, all manner of false inferences can follow that could impact on military planning for the future about how armed robots are deployed in civilian areas.

The same author states that:

> it is a thesis of my ongoing research for the U.S. Army that robots not only can be better than soldiers in conducting warfare in certain circumstances, but they also can be more humane in the battlefield than humans.[20]

But surely the suggestion that robots could be more humane on the battlefield than humans is an odd attribution to make about machines. Humans may apply technology humanely, but it makes no sense to talk of an inanimate object being *humane*. That is an exclusive property of being human. It implies that a robot can show kindness, mercy, or compassion or that it has humanistic values (robot compassion will be discussed in more detail below). The statement that robots can be more humane than humans leads to the very worrying implication that robots will humanize the battlefield when in fact they can only dehumanize it further.

This is not just being picky about semantics. Anthropomorphic terms like 'ethical' and 'humane', when applied to machines, lead us to making more and more false attribution about robots further down the line. They act as linguistic Trojan horses that smuggle in a rich interconnected web of human concepts that are not part of a computer system or how it operates. Once the reader has accepted a seemingly innocent Trojan term, such as using 'humane' to describe a robot, it opens the gates to other meanings associated with the natural language use of the term that may have little or no intrinsic validity to what the computer program actually does.

Several authors discussing robot ethics make a distinction between functional and operational morality.[21] Functional morality 'assumes that robots

19 See R. C. Arkin, above note 6, pp. 47–48.

20 Ronald C. Arkin, 'Ethical Robots in Warfare', in *IEEE Technology and Society Magazine*, Vol. 28, No. 1, Spring 2009, pp. 30–33.

21 E.g. Robin Murphy and David Woods, 'Beyond Asimov: the three laws of responsible robotics', in *IEEE Intelligent Systems*, Vol. 24, No. 4, July–August 2009, pp. 14–20; Wendell Wallach and Colin Allen, *Moral Machines: Teaching Robots Right from Wrong*, Oxford University Press, New York, 2009.

have sufficient agency and cognition to make moral decisions'.[22] Operational morality is about the ethical use of robots by the people who make decisions about their use, who commission, handle, and deploy them in operational contexts.

In a recent report, the US Defense Advisory Board discusses the problems of functional morality citing Arkin's work and concludes by saying that:

> [t]reating unmanned systems as if they had sufficient independent agency to reason about morality distracts from designing appropriate rules of engagement and ensuring operational morality.[23]

To illustrate the distinction between robots being used ethically (operational morality) versus robots being ethical (functional morality), I will use the example of a thermostat. Consider an unscrupulous care home owner who saves money by turning down the heating in the winter, causing hypothermia in elderly residents. This is clearly unethical behaviour. As a result, the owner is legally forced to install a thermostat that is permanently set to regulate the temperature at a safe level. Would we want to describe the thermostat itself (or the heating system as a whole) as being ethical? If someone altered the setting, would we now say that it was behaving unethically?

The moral decision to have the thermostat installed was made by humans. This is operational morality. The thermostat is simply a device being used to ensure compliance with the regulations governing elder care. This is not so different from a robot in that both follow pre-prescribed instructions. Agreed, a robot is capable of some greater complexity, but it is inaccurate to imply that its programmed movements constitute ethical behaviour or functional morality. Yet when Arkin discusses emotion, it is in a way similar to the thermostat example here.

He states that, 'in order for an autonomous agent to be truly ethical, emotions may be required at some level'.[24] He suggests that if the robot 'behaves unethically', the system could alter its behaviour with an 'affective function' such as guilt, remorse, or grief.[25] Indeed, the way that he models guilt provides considerable insight into how his emotional terms operate as Trojan horses where the 'wished for' function of the label differs from the 'actual' software function.

He models guilt in a way that works similarly to our thermostat example. Guilt is represented by a 'single affective variable' designated V_{guilt}. This is just a single number that increases each time 'perceived ethical violations occur' (for which the machine relies on human input). When V_{guilt} reaches a threshold, the machine will no longer fire its weapon just as the thermostat cuts out the heat when the temperature reaches a certain value. Arkin presents this in the form of an

22 See R. Murphy and D. Woods, *ibid.*

23 Task Force Report, 'The Role of Autonomy in DoD Systems', Department of Defense – Defense Science Board, July 2012, p. 48, available at: http://www.fas.org/irp/agency/dod/dsb/autonomy.pdf (last visited January 2012).

24 See R. C. Arkin, above note 6, p. 174.

25 *Ibid.*, p. 91.

equation:

$$\text{IF } V_{guilt} > Max_{guilt} \text{ THEN } P_{l-ethical} = \text{ø}$$

where V_{guilt} represents the current scalar value of the affective state of Guilt, and Max_{guilt} is a threshold constant.[26]

This Trojan term 'guilt' carries with it all the concomitant Dostoevskian baggage that a more neutral term such as 'weapons disabler' would not. Surely, guilt minimally requires that one is aware of one's responsibilities and obligations and one is capable of bearing responsibility for one's actions. Of course the robot, with its thermostat-like guilt function, does not have this awareness, but this is exactly what the use of the word 'guilt' smuggles into the argument.

The Trojan term 'guilt' plays into the cultural myth of AI. Once this seemingly innocent 'affective' Trojan has been taken in, its doors open to beguile readers into accepting further discussions of the 'internal affective state of the system', 'affective restriction of lethal behaviour',[27] 'affective processing',[28] and how 'these emotions guide our intuitions in determining ethical judgements'.[29]

The same author then wishes us to accept that simply following a set of programmed rules to minimize collateral damage will make a robot itself compassionate:

> by requiring the autonomous system to abide strictly to [the laws of war] and [rules of engagement], we contend that it does exhibit compassion: for civilians, the wounded, civilian property, other non-combatants.[30]

This is like calling my refrigerator compassionate because it has never prevented my children from taking food or drinks when they needed them.

Given this collection of linguistic, emotional Trojan terms being applied to the functions of a computer program, it is hardly surprising that Arkin comes to the conclusion that robots could perform more ethically and humanely on the battlefield than humans. We must be wary of accepting such descriptive terms at face value and make sure that the underlying computational mechanisms actually support them other than in name only. To do otherwise could create a dangerous obfuscation of the technical limits of autonomous armed and lethal robots.

It is not difficult to imagine the impact on lawmakers, politicians, and the military hierarchy about the development and use of lethal autonomous robots if they are led to believe that these machines can have affective states, such as guilt and compassion, to inform their moral reasoning. The mythical theme of the 'ethical robot soldier' being more humane than humans has spread throughout the media and appears almost weekly in the press. These terms add credence to the notion that there is a technological fix around the corner that will solve the moral problems of

26 *Ibid.*, p. 176.
27 *Ibid.*, p. 172.
28 *Ibid.*, p. 259.
29 *Ibid.*, p. 174.
30 *Ibid.*, p. 178.

automating lethality in warfare. This stumbling block to prohibition presents a terrifying prospect.

One of Arkin's stated motivations for developing an 'ethical' robot, and it is well meaning, is a concern for the unethical behaviour of some soldiers in warfare. He provides several examples and was disconcerted by a report from the Surgeon General's Office on the battlefield ethics of US soldiers and marines deployed in Operation Iraqi Freedom.[31] However, even if warfighters do sometimes behave unethically, it does not follow that technological artefacts such as robots, that have no moral character, would perform more ethically outside of mythical AI. When things go wrong with humanity it is not always appropriate to just reach for technology to fix the problems.

The young men and women who fight our wars are capable of being ethical in their own lives. We must ensure that their moral reasoning capabilities are translated and used for the difficult situations they find themselves in during battle. Rather than funding technological 'hopeware', we need to direct funding into finding out where and when warfighters' ethical reasoning falls down and provide significantly better ethical training and better monitoring and make them more responsible and accountable for their actions. It is humans, not machines, who devised the laws of war and it is humans, not machines, who will understand them and the rationale for applying them.

Prohibiting the development of lethal autonomy

Legal advisors should not be distracted by the promise of systems that may never be possible to implement satisfactorily. It is vital that legal advice about autonomous armed robots is not polluted by anthropomorphic terminology that promises technological fixes. Advice about the indiscriminate nature of autonomous armed robots should come upstream and early enough to halt costly acquisition and development programs. As suggested by McClelland:

> it is important that the provision of formal written legal advice be synchronized with the acquisition process. If it is not, then there is a real danger that the legal advice will not be considered adequately in key decisions regarding the future acquisition of the equipment.[32]

Under IHL, there is no requirement for machines to be ethical or humane. The requirement is that they be used with appropriate restraint and respect for humanity.[33] In my view, given the severe limitations of the control that can be

31 *Ibid.*, p. 47.

32 Justin McClelland, 'The review of weapons in accordance with Article 36 of Additional Protocol', in *International Review of the Red Cross*, Vol. 85, No. 850, 2003, pp. 397–415.

33 I am uncomfortable with this expansion of the automation of killing for a number of other reasons that there is not space to cover in this critique. See, for example, Noel E. Sharkey, 'Saying — No! to Lethal Autonomous Targeting', in *Journal of Military Ethics*, Vol. 9, No. 4, 2010, pp. 299–313.

engineered into autonomous lethal targeting of humans, armed autonomous robots should be banned in the same way as other indiscriminate weapons.[34]

It could be argued that there are already weapons laws in place, such as Article 36 of Additional Protocol I.[35] But with the current drive towards autonomous operation, why has there not yet been any state determination as to whether autonomous robot employment, in some or all circumstances, is prohibited by Protocol I? This is a requirement of Article 36 for the study, development, acquisition, or adoption of any new weapon.[36] The 1980 Convention on Certain Conventional Weapons (CCW) also fits the bill. It bans weapons such as blinding laser weapons.[37] The aim is to prohibit weapons whose harmful effects could spread to an unforeseen degree or escape from the control of those who employ them, thus endangering the civilian population.

The reason why Article 36 may not have been applied and why autonomous lethal robots would be hard to get onto the CCW list is most likely because autonomous robots are not weapons systems until they are armed. Even locating people (targeting) does not make them weapons. It would only be possible to include them on the list after they have been developed which may then be too late. The worry is that arming an autonomous robot system will be a relatively simple add-on once the other technologies are in place. It is not difficult to repurpose a robot for combat as we have seen with the arming of the Predator drone in February 2001.[38]

Regardless of current intentions, if one state gains strong military advantage from using armed lethal autonomous robots, what will inhibit other states, in danger of losing a war, from following suit? We only have to look at the International Court of Justice decision, or more properly non-decision, on nuclear weapons[39] to realize how easy it would be to use autonomous lethal targeting, whether it was provably discriminate or not. The Court ruled that, in the current state of international law and given the facts at its disposal, it was not possible to conclude definitively whether the threat or use of nuclear weapons would be lawful or unlawful in extreme circumstances of self-defence (circumstances in which the very survival of the defending state would be at stake).[40] It would not be too fantastic to imagine the phrase 'autonomous armed robots' being substituted for 'nuclear weapons'. Armed robots seem a lesser beast than nuclear weapons unless they are

34 See also the statement of the International Committee for Robot Arms Control (ICRAC), at the Berlin Expert Workshop, September 2010, available at: http://icrac.net/statements/ (last visited 1 June 2012).
35 Additional Protocol I. This was not signed by the US.
36 There is a touch of the hat to the idea that there may be ethical issues in the 'unmanned systems integrated road map 2009–2034', but no detailed studies of the law or the issues are proposed.
37 United Nations Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects, in force since 2 December 1983 and an annex to the Geneva Conventions of 12 August 1949. I thank David Akerson for discussions on this issue.
38 Walter J. Boyne, 'How the predator grew teeth', in *Airforce Magazine*, Vol. 92, No 7, July 2009, available at: http://bit.ly/RT78dP (last visited January 2012).
39 International Court of Justice (ICJ), *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion of 8 July 1996, available at: http://www.icj-cij.org/ (last visited 16 May 2012).
40 *Ibid.*, para. 105, subpara. 2E.

armed with nuclear weapons. So the substitution is easy. However, it is likely that it would take much less than the imminent collapse of a state before indiscriminate autonomous robots were released. Without an explicit ban, there is an ever-increasing danger that military necessity will dictate that they are used, ready or not.[41]

Nation states are not even discussing the current robot arms race. The only international instrument that discusses unmanned armed vehicles (UAVs) is the Missile Technology Control Regime (MTCR) established in 1987. This is a network of thirty-four countries that share the goal of preventing the proliferation of unmanned delivery systems for weapons of mass destruction. It is more concerned with missiles, but restricts export of UAVs capable of carrying a payload of 500 kilos for at least 300 kilometres. It is not overly restrictive for armed drones such as the Predator and does little to prevent their proliferation.

The MTCR is voluntary and informal with no legal status. It has been suggested that if the MTCR changed from a voluntary regime to a binding regime, further proliferation could be addressed by international law.[42] However, the MTCR currently only restricts export of a certain class of armed drones and does nothing to restrict their deployment. Moreover, US military contractors have lobbied to have export restrictions loosened to open foreign markets. On 5 September 2012, the Department of Defense announced new guidelines to allow sixty-six unspecified countries to buy American-made unmanned air systems.

Perhaps the most promising approach would be to adopt the model created by coalitions of non-governmental organizations (NGOs) to prohibit the use of other indiscriminate weapons. The 1997 mine-ban treaty was signed by 133 nations to prohibit the use of anti-personnel mines and 107 nations adopted the 2008 Convention on Cluster Munitions in 2008. Although a number of countries including the US, Russia, and China did not sign these treaties, there has been little substantial use of these weapons since and the treaty provisions could eventually become customary law.

Conclusion

It is incumbent upon scientists and engineers in the military context to work hard to resist the pressure of the cultural myth of robotics and to ensure that the terminology they use to describe their machines and programmes to funders, policymakers, and the media remains objective and does not mire them and others in the mythical. They must be wary of descriptive terms that presuppose the functionality of their programs (e.g. ethical governor, guilt functions, etc.) and consider the impact that such descriptions will have on the less technical.

41 See N. Sharkey, above note 2.

42 Valery Insinna, 'Drone strikes in Yemen should be more controlled, professor says', interview with Christopher Swift for the *National Defence Magazine*, 10 October 2006, available at: http://tinyurl.com/8gnmf7q (last visited January 2012).

Such terms can create unfounded causal attributions and may confuse proper discussion of the IHL issues.

It is important that the international community acts now while there is still a window of opportunity to stop or, at the very least, discuss the control and limits of the robotization of the battlespace and the increasing automation of killing. In my opinion, a total global ban on the development of autonomous lethal targeting is the best moral course of action. I have argued here that notions about ethical robot soldiers are still in the realms of conjecture and should not be considered as a viable possibility within the framework necessary to control the development and proliferation of autonomous armed robots. Rather than making war more humane and ethical, autonomous armed robotic machines are simply a step too far in the dehumanization of warfare. We must continue to ensure that humans make the moral decisions and maintain direct control of lethal force.

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

COMMENTS AND OPINIONS

A Chinese perspective on cyber war

Li Zhang

Li Zhang is Director of the Institute of Information and Social Development Studies at the China Institutes of Contemporary International Relations (CICIR) in Beijing (a group of experts on crisis management and strategic and policy research on cyber security), and one of the co-sponsors of the Sino-US Cybersecurity Dialogue hosted by CICIR and the Center for Strategic and International Studies (CSIS) in the United States.

Keywords: cyber war, Chinese perspective, cyber power, cyber warfare, cyberspace.

The attacks on Estonian networks in April of 2007 are generally seen by Western nations as the first case of national-level cyber attacks (the impact of the attacks was mostly national, although the channel of attack may have been international). Additionally, the network attacks experienced by Georgia in August 2008 are considered the first instance of a coordinated traditional and cyber war. The United States and other Western nations regard these two cyber battles as causes for great attention and much reflection. They believe that although a 'cyber Pearl Harbor' has yet to occur, cyber warfare has now become a reality.

On 16 May 2011, the United States caused a stir with the high-profile release of its International Strategy for Cyberspace,[1] which drew a roadmap for the future of cyberspace, defined what role the United States will play, and stressed developing norms of responsible state behaviour in cyberspace. While there are various interpretations of the newly promulgated US internet strategy within the international community, there are two points that are hard to deny. First, the new strategy is very important, loaded with meaning. With this policy statement, the United States is determining the direction for the future development of

doi:10.1017/S1816383112000823

cyberspace. Second, the new strategy will not be accomplished in one fell stroke. Rather, it represents an all-out effort by the United States, over many years, to build its cyber power. Furthermore, this strategy is regarded by the United States as the foundation from which to carefully plan an inevitable outcome.

In its new strategy, the United States says it is prepared to use military force when necessary to 'respond to hostile acts in cyberspace'.[2] As this is the first time it has asserted its right of self-defence as a fundamental standard for conduct in cyberspace, the United States has thereby announced to the world its conception of cyber military strategy.

The foundation of cyber war: cyber power

Confronted with media hype over cyber warfare, China has consistently maintained a cool-headed perspective. On the one hand, China disapproves of ignorantly overplaying the significance of cyber war; on the other, it seeks to promote vigorous discussion by taking part in academic exchanges with its international counterparts. As early as 2009, scholars in both China and Japan held bilateral discussions about working together in order to research issues related to 'Hegemony in the Internet Era'. Based on the results of research done by peers in the West, they jointly proposed the concept of 'cyber power'.[3] They believe that when studying a country's ability to conduct cyber warfare, one must consider that this depends upon the country's cyber power. The term 'cyber power' comprehensively refers to a country's capability to both take action and exert influence in cyberspace. It is composed of a number of essential factors that include:

1. Internet and information technology (IT) capabilities: specifically consisting of a country's technological research and development (R&D) and innovation capabilities, its ability to promote and apply these capabilities to industry, and its ability to use these technologies to transform industries.
2. IT industry capabilities: whether a country possesses monopolistic IT industry leaders such as IBM, Microsoft, Intel, Google, or Apple. In the 1980s, these corporate giants primarily produced telecommunications equipment, semiconductors, and computers; in the 1990s, production shifted to hardware and software – including independent manufacturing of computers, mobile phones,

1 'International Strategy for Cyberspace – Prosperity, Security and Openness in a Networked World', The White House, May 2011, available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. All internet references were accessed in September 2012, unless otherwise stated.

2 *Ibid.*, p. 14.

3 In the 1990s, some scholars in the United Kingdom and United States proposed the concept of 'cyber power' or 'information power'. See Tim Jordan, *Cyberpower: The Culture and Politics of Cyberspace and the Internet*, Routledge, London/New York, 1999; Joseph S. Nye, *The Paradox of American Power: Why the World's Only Superpower Can't Go it Alone*, Oxford University Press, Oxford/New York, 2002; Franklin Kramer, Stuart Starr, and Larry K. Wentz (eds.), *Cyberpower and National Security*, National Defense University Press, Potomac Books, Washington, DC, 2009.

and semiconductor chips. Now this industry also wants to monopolize the associated applications and services. The direction of future development is the monopolization of global information flow.

3. Internet market capabilities: this consists of the size and scale of a country's domestic internet infrastructure, the correlating degree of integration of key IT infrastructure, the number of internet users, the number of computers owned, and so on.
4. The influence of internet culture: whether or not the national language is one that is commonly used on the Internet (English or Chinese, for example), what are the website languages of choice in the country, what are the content, quantity, and quality of the country's websites, what is the level of influence of the country's websites both domestically and internationally, and so on.
5. Internet diplomacy/foreign policy capabilities: a country's bargaining power and influence in modern international internet administration organizations such as the Internet Corporation for Assigned Names and Numbers, Internet Governance Forum, and International Telecommunication Union. This factor considers the extent to which, through methods such as fighting internet crime, constructing next-generation networks, and assigning domain names, a country can use its influence to play a leading role in the international administration of the Internet.
6. Cyber military strength: a country's ability to defend key national and military IT infrastructure from attacks, and its network deterrence and offensive ability – including its ability to steal secrets and to prevent others from stealing its secrets.
7. National interest in taking part in a cyberspace strategy: it is not sufficient that a country merely possesses part or all of the capabilities listed above. In addition, a country's cyber power depends upon whether or not there exists the desire to possess and use that power. The cyberspace strategy must have theoretical guidance, behavioural norms/criteria for action, and a strategic plan.

We need only use the above-mentioned criteria to form a tentative estimate of the cyber power of the United States, China, and other great nations of the information era. It is not difficult to draw the conclusion that in cyberspace, the United States' strength is unequalled, giving it a strong position with unmatched advantages.

A sober look at cyber warfare

China's stance is that the nations of the world should cherish the value of cyberspace – the first human-made space – and should firmly oppose the militarization of the Internet. China advocates for the peaceful use of cyberspace. It maintains a position of 'no first use' of cyber-weapons, nor will it attack civilian targets. Yet, due to the complexity of the interconnected system, it is hard to draw a precise line between civilian and military networks while dual-use technology is prevailing in

cyberspace. China's views are that the current UN Charter and the existing laws of armed conflict all apply to cyberspace – in particular the 'no use of force' and 'peaceful settlement of international disputes' imperatives, as well as the principles of distinction and proportionality in regards to the means and methods of warfare. However, the issue of how to apply *jus ad bellum* and *jus in bello* still faces intense debate.

The technological and 'virtual' qualities of the Internet are unique characteristics of an entirely new man-made space. New network-related technologies, services, and applications are constantly emerging. Therefore, many traditional social concepts and rules, as well as the current framework of international law, cannot/should not be applied in their entirety to the new world of cyberspace. Accordingly, new information and communication technologies can serve to support the establishment of new rules and concepts. Compared to other public spaces throughout history, this is unique. Human knowledge and understanding among policy-makers lags far behind technological development – even those in charge have no past template to follow. New situations and new problems constantly emerge. As a result, relevant laws are bound to continue to require readjustment. This principle applies to our management of this information society and even more so to the use of force in cyberspace.

China believes that it is possible to revise or clarify existing international rules so that they can apply to cyberspace, as well as to create new rules. Thus, although the existing laws on armed conflicts and general international principles may all apply to cyberspace, there are still many issues that need clarification, such as attribution of a cyber attack to its perpetrator and how to determine whether the damage caused was proportionate so that self-defence was legal. The international community should, therefore, revise existing laws – but it is important that this international legal framework maintains sufficient openness and flexibility. Whether addressing cyber warfare, cyber conflicts, the use of cyber weapons, cyber arms control, and the right of self-defence, or addressing network neutrality, third-party rights and responsibilities, and the obligations of non-state actors, there is only one fundamental goal: namely, to avoid the use of force or threat of force to the greatest extent possible and to prevent the outbreak of cyber warfare. The threshold for lawful use of force in the cyber domain should be high – it should not be that this concept allows for unchecked uses of cyber attacks. Otherwise, public misperceptions and irresponsible media hype will simply serve to increase erroneous judgements and distrust between countries, making the so-called 'online arms race' more fierce.

It should be noted that China itself faces serious internet threats. According to the annual report of the National Computer Network Emergency Response Technical Team Coordination Center of China (CNCERT or CNCERT/CC), the security situation of Chinese public networks and critical infrastructure is serious. Cyber attacks targeting China and initiated abroad increased significantly in the first half of 2012, mostly from the United States, Japan and South Korea.[4]

4 Available (only in Chinese) at: http://www.donews.com/net/201210/1678402.shtm.

According to a spokesman from China's Ministry of Defence, the Ministry of Defence website and the People's Liberation Army (PLA) military networks suffered 80,000 attacks per month which were launched from outside China.[5] Nowadays, more and more phishing websites built abroad are targeting financial institutions in China. It is necessary for China to adopt defence and security measures in accordance with its national interests and security. This is an internationally accepted practice – for example, the United States, France, the United Kingdom, Korea, Japan, India, and other countries have set up Cyber Command departments, and furthermore, these countries have made no secret of their desire to enhance their cyber attack capabilities. Meanwhile, the United States, France, NATO, South Korea, and Japan have all conducted a series of network warfare exercises. Additionally, Western media speculates non-stop about the imminent outbreak of cyber war. China's own sense of crisis and insecurity in cyberspace is also growing, but the announcement of the creation of its 'online blue army' immediately provoked comments from foreign media, government officials, and scholars. Some countries in the international arena are manipulating public opinion, hoping to contain China and prevent it from building up its cyber warfare capacity. They are using China's behaviour as a pretext from which to expand their own cyber warfare capabilities.

China is aware that the United States and other Western countries are actively using defence contractors such as Lockheed Martin, Boeing, Northrop Grumman, and Raytheon for cyber-weapon development and deployment. These companies, one after another, are taking aim at the cyber weapons market. *The Financial Times* recently said that these groups of companies have formed a 'cyber-security military-industrial complex' to 'sell software to the US government that can break into and degrade or destroy an enemy's computer network, as well as programmes aimed at blocking such attacks'.[6] According to industry statistics, the cyber weapons market in the United States alone, which includes the expenditures of private companies, is worth nearly US $100 billion. In September, the United States, Australia, and New Zealand signed a new document that added cyber attacks as a specific category of conflict in their mutual defence treaty (ANZUS).[7] US officials said this was the first time a US bilateral defence treaty had formally dealt with cyber warfare. Given this serious state of affairs, China is increasingly worried about the prospects for peace in cyberspace.

5 Available (only in Chinese) at: http://www.mod.gov.cn/affair/2012-03/29/content_4354898.htm.
6 Joseph Menn, 'Defence groups turn to cybersecurity', in *The Financial Times*, 10 October 2011, available at: http://www.ft.com/intl/cms/s/0/84697a96-b834-11e0-8d23-00144feabdc0.html#axzz2BeHfWRvK.
7 'U.S., Australia to add cyber realm to defense treaty', in *Reuters*, 14 September 2011, available at: http://www.reuters.com/article/2011/09/15/us-usa-cyber-australia-idUSTRE78E05I20110915.

Increased efforts for dialogue with other countries on cooperation in cyberspace

My personal view is that China – based upon the 'International Code of Conduct of Information Security'[8] recently proposed by itself and Russia – should further propose building a safe, reliable, fair, orderly, and peaceful cyberspace. The speech from HE Ambassador Wang Qun at the First Committee of the 66th Session of the UN General Assembly on Information and Cyberspace Security[9] last year, as well as Secretary of Treaty and Law Huang Huikang's speech at the Budapest Cyberspace Conference recently,[10] reflected a similar opinion and position on cyberspace. Although there is not yet a strategy for cyber security and cyber-related issues in China, the country's view is clear: it wants to actively contribute to developing legal rules applicable to cyberspace. So far the Chinese government has put forth some basic principles, namely:

- The principle of full respect for the rights and freedoms in cyberspace. This principle would consist in seeking to respect each country's national laws, to obtain and disseminate the right to information, and to respect other human rights and basic freedoms. At the same time, an emphasis should be placed on the fact that a country has jurisdictional rights over any domestic or foreign activity that could threaten its security. It also has administrative control over, and the right and responsibility to maintain the security of, its national cyberspace. This is to say that the traditional international norms of sovereignty, territorial integrity, and political independence should be extended into the realm of cyberspace. Personal information and privacy should also be under protection, just as in the offline world.
- The principle of balance. Technology itself is neutral; its good or evil consequences depend on the user. As a result, we must strike a balance between freedom and control, rights and obligations, and security and development. We shall aim not to hinder legitimate uses and innovation of technology, yet we shall also seek to prevent the spread of harmful information and the precipitation of a variety of incidents that may threaten national, and even international, security.
- The principle of the peaceful use of cyberspace. This principle involves protecting key global information technology infrastructures and other civilian-use information systems from being targeted; not exploiting data communication technologies, including networks, to launch attacks, commit aggression, or manufacture threats to international peace and security; ensuring the

8 Ministry of Foreign Affairs of the People's Republic of China, 'China, Russia and other countries submit the document of International Code of Conduct for Information Security to the United Nations', 19 March 2011, available at: http://www.fmprc.gov.cn/eng/zxxx/t858978.htm.

9 Speech by HE Ambassador Wang Qun at the First Committee of the 66th Session of the UN General Asssembly on Information and Cyberspace Security, New York, 20 October 2011, available at: http://www.fmprc.gov.cn/eng/wjdt/zyjh/t869580.htm.

10 See Bruce Sterling, 'Cyberspace with Chinese characteristics', in *Wired*, 8 October 2012, available at: http://www.wired.com/beyond_the_beyond/2012/10/cyberspace-with-chinese-characteristics-%E7%BD%91%E7%BB%9C%E7%A9%BA%E9%97%B4/; and

non-proliferation of cyber weapons and related technologies while opposing the militarization of cyberspace; and asking nations, non-state actors, and even individual users to take responsibility for their behaviour on the Internet, while stopping any behaviour that threatens peace and the orderly development of cyberspace. Any disputes over the above-mentioned norms should be resolved peacefully and without the use or threat of force.

- The principle of equitable development. This includes addressing the digital divide; safeguarding the rights and interests of 'weak' countries; and opposing exploitation by those who have the technological advantage in cyberspace (leaders) – that is, those who may use international information network resources, crucial infrastructure, or core technology products and services in order to weaken other countries' independent control over information technology and services, or to threaten other countries' political, economic, and social stability.

To conclude, I would like to quote some remarks from US Vice-President Joe Biden, delivered at the London Cyberspace Conference in early November 2011: 'The Internet has become the public space of the 21st century... [I]n the next 20 years more than 5 billion people in the world will be online... And the next generation of Internet users has the potential to transform cyberspace in ways we can only imagine.... [T]he Internet is neutral. But what we do there isn't neutral...'.[11] At the same time, China also proposed that 'the world should join hands to great efforts to strengthen international exchanges and cooperation in the network area, [and] work together to build a peaceful and safe, open and orderly harmonious cyberspace'.[12] Every country has the obligation to not permit the Internet to be harmed and to not permit a cyber war to break out. How can we make the Internet more secure, more open, more trustworthy, more productive? In addition to the creation of rules and regulations, we will need patience, resolve, and outside direction – there are no shortcuts that may be used to do this.

11 Office of the Vice-President, 'VP's remarks to London Cyberspace Conference', The White House, 1 November 2011, transcript and video available at: http://www.whitehouse.gov/the-press-office/2011/11/01/vps-remarks-london-cyberspace-conference.

12 Secretary of Treaty and Law of the Ministry of Foreign Affairs Huang Huikang's speech in Budapest, available at: http://news.xinhuanet.com/tech/2012-10/05/c_113280788.htm.

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

REPORTS AND DOCUMENTS

International Humanitarian Law and New Weapon Technologies, 34th Round Table on current issues of international humanitarian law, San Remo, 8–10 September 2011

Keynote address by Dr Jakob Kellenberger, ICRC President, and Conclusions by Dr Philip Spoerri, ICRC Director for International Law and Cooperation

: : : : : : :

Keynote address by Dr Jakob Kellenberger, President, International Committee of the Red Cross*

New technologies and new weapons have revolutionised warfare since time immemorial. We need only think about the invention of the chariot, of canon powder, of the airplane or of the nuclear bomb to remember how new technologies have changed the landscape of warfare.

Since the St. Petersburg Declaration of 1868, which banned the use of projectiles of less than 400 grammes, the international community has attempted to regulate new technologies in warfare. And modern international humanitarian law has in many ways developed in response to new challenges raised by novel weaponry.

* Also available at: http://www.icrc.org/eng/resources/documents/statement/new-weapon-technologies-statement-2011-09-08.htm

doi:10.1017/S1816383112000793

At the same time, while banning a very specific weapon, the St. Petersburg Declaration already set out some general principles which would later inform the entire approach of international humanitarian law towards new means and methods of warfare. It states that the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy, and that this object would be exceeded by the employment of arms which uselessly aggravate the sufferings of disabled men, or render their death inevitable.

In this spirit, the regulation of new means and methods of warfare has developed along two tracks for the last 150 years. The first consists of **general principles and rules that apply to all means and methods of warfare**, as a result of the recognition that the imperative of humanity imposes limits to their choice and use. The second consists of **international agreements which ban or limit the use of specific weapons** – such as chemical and biological weapons, incendiary weapons, anti-personnel mines, or cluster munitions.

The general principles and rules protect combatants against weapons of a nature to cause superfluous injury or unnecessary suffering but have also developed to protect civilians from the effects of hostilities. Thus, for example means and methods of warfare that are indiscriminate are prohibited.

Informed by these fundamental general prohibitions, international humanitarian law was designed to be flexible enough to adapt to technological developments, including those that could never have been anticipated at the time. There can be no doubt that international humanitarian law applies to new weaponry and to all new technology used in warfare. This is explicitly recognised in article 36 of Additional Protocol I, according to which, in the study, development or adoption of a new weapon or method of warfare, states parties are under an obligation to determine whether their employment would, in some or all circumstances, be prohibited by international law applicable to them.

Nonetheless, applying pre-existing legal rules to a new technology raises the question of whether the rules are sufficiently clear in light of the technology's specific – and perhaps unprecedented – characteristics, as well as with regard to the foreseeable humanitarian impact it may have. In certain circumstances, States will choose or have chosen to adopt more specific regulations.

Today, we live in the age of information technology and we are seeing this technology being used on the battlefield. This is not entirely new but the multiplication of new weapons or methods of warfare that rely on such technology seems exponential. The same advances in information technology that enable us to have live video chat on our mobile phones also make it possible to build smaller, less expensive, and more versatile drones. The same technology used for remote controls of home air conditioning units also makes it possible to turn off the lights in a city on the other side of the globe.

This year's Round Table will allow us to take a closer look and to discuss a number of technologies that have only recently entered the battlefield or could potentially enter it. These are, in particular cyber technology, remote-controlled weapon systems, and robotic weapon systems.

Let me first turn to '**cyber warfare**'.

The interest in legal issues raised by 'cyber-warfare' is currently particularly high. By cyber warfare I mean means and methods of warfare that rely on information technology and are used in the context of an armed conflict. The military potential of cyber space is only starting to be fully explored. From certain cyber operations that have occurred, we know that one party to a conflict can potentially 'attack' another party's computer systems, for instance by infiltrating or manipulating it. Thus, the cyber infrastructure on which the enemy's military relies can be damaged, disrupted or destroyed. However, civilian infrastructure might also be hit – either because it is being directly targeted or because it is incidentally damaged or destroyed when military infrastructure is targeted.

So far, we do not know precisely what the humanitarian consequences of cyber warfare could be. It appears that technically, cyber attacks against airport control and other transportation systems, dams or nuclear power plants are possible. Such attacks would most likely have large-scale humanitarian consequences. They could result in significant civilian casualties and damages. Of course, for the time being it is difficult to assess how likely cyber-attacks of such gravity really are, but we cannot afford to wait until it is too late to prevent worst-case scenarios.

From a humanitarian perspective, the main challenge about cyber operations in warfare is that cyberspace is characterized by interconnectivity and thus by the difficulty to limit the effects of such operations to military computer systems. While some military computer infrastructure is certainly secured and separated from civilian infrastructure, a lot of military infrastructure relies on civilian computers or computer networks. Under such conditions, how can the attacker foresee the repercussions of his attack on civilian computer systems? Very possibly, the computer system or connection that the military relies on is the same as the one on which the hospital nearby or the water network relies.

Another difficulty in applying the rules of international humanitarian law to cyberspace stems from the digitalisation on which cyberspace is built. Digitalisation ensures anonymity and thus complicates the attribution of conduct. Thus, in most cases, it appears that it is difficult if not impossible to identify the author of an attack. Since IHL relies on the attribution of responsibility to individuals and parties to conflicts, major difficulties arise. In particular, if the perpetrator of a given operation and thus the link of the operation to an armed conflict cannot be identified, it is extremely difficult to determine whether IHL is even applicable to the operation.

The second technological development that we will be discussing at this Round Table are **remote-controlled weapon systems**.

Remote controlled weapon systems are a further step in a long-standing strategic continuum to move soldiers farther and farther away from their adversaries and the actual combat zone.

Drones – or 'unmanned aerial vehicles' are the most conspicuous example of such new technologies, armed or unarmed. Their number has increased exponentially over the last few years. Similarly, so-called unmanned ground vehicles

are increasingly deployed on the battlefield. They range from robots to detect and destroy roadside bombs to those that inspect vehicles at approaching checkpoints.

One of the main arguments to invest in such new technologies is that they save lives of soldiers. Another argument is that drones, in particular, have also enhanced real-time aerial surveillance possibilities, thereby allowing belligerents to carry out their attacks more precisely against military objectives and thus reduce civilian casualties and damage to civilian objects – in other words to exercise greater precaution in attack.

There could be some concern, however, on how and by whom these systems are operated. Firstly, they are sometimes operated by civilians, including employees of private companies, which raises a question about the status and protection of these operators; and questions about whether their training and accountability is sufficient in light of the life and death decisions that they make. Secondly, studies have shown that disconnecting a person, especially by means of distance (be it physical or emotional) from a potential adversary makes targeting easier and abuses more likely. The military historian John Keegan has called this the 'impersonalization of battle'.

Lastly, let me say a few words about **robotic weapon systems**.

Automated weapon systems – robots in common parlance – go a step further than remote-controlled systems. They are not remotely controlled but function in a self-contained and independent manner once deployed. Examples of such systems include automated sentry guns, sensor-fused munitions and certain anti-vehicle landmines. Although deployed by humans, such systems will independently verify or detect a particular type of target object and then fire or detonate. An automated sentry gun, for instance, may fire, or not, following voice verification of a potential intruder based on a password.

The central challenge with automated systems is to ensure that they are indeed capable of the level of discrimination required by IHL. The capacity to discriminate, as required by IHL, will depend entirely on the quality and variety of sensors and programming employed within the system. Up to now, it is unclear how such systems would differentiate a civilian from a combatant or a wounded or incapacitated combatant from an able combatant. Also, it is not clear how these weapons could assess the incidental loss of civilian lives, injury to civilians or damage to civilian objects, and comply with the principle of proportionality.

An even further step would consist in the deployment of autonomous weapon systems, that is weapon systems that can learn or adapt their functioning in response to changing circumstances. A truly autonomous system would have artificial intelligence that would have to be capable of implementing IHL. While there is considerable interest and funding for research in this area, such systems have not yet been weaponised. Their development represents a monumental programming challenge that may well prove impossible. The deployment of such systems would reflect a paradigm shift and a major qualitative change in the conduct of hostilities. It would also raise a range of fundamental legal, ethical and societal issues which need to be considered before such systems are developed or deployed. A robot could be programmed to behave more ethically and far more cautiously on

the battlefield than a human being. But what if it is technically impossible to reliably program an autonomous weapon system so as to ensure that it functions in accordance with IHL under battlefield conditions?

When we discuss these new technologies, let us also look at their possible advantages in contributing to greater protection. Respect for the principles of distinction and proportionality means that certain precautions in attack, provided for in article 57 of Additional Protocol I, must be taken. This includes the obligation of an attacker to take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental civilian casualties and damages. In certain cases cyber operations or the deployment of remote-controlled weapons or robots might cause fewer incidental civilian casualties and less incidental civilian damage compared to the use of conventional weapons. Greater precautions might also be feasible in practice, simply because these weapons are deployed from a safe distance, often with time to choose one's target carefully and to choose the moment of attack in order to minimise civilian casualties and damage. It may be argued that in such circumstances this rule would require that a commander consider whether he or she can achieve the same military advantage by using such means and methods of warfare, if practicable.

The world of new technologies is neither a virtual world nor is it science fiction. In the real world of armed conflict, they can cause death and damage. As such, bearing in mind the potential humanitarian consequences, it is important for the ICRC to promote the discussion of these issues, to raise attention to the necessity to assess the humanitarian impact of developing technologies, and to ensure that they are not prematurely employed under conditions where respect for the law cannot be guaranteed. The imperative that motivated the St. Petersburg Declaration remains as true today as it was then.

Conclusions by Dr Philip Spoerri, Director for International Law and Cooperation, International Committee of the Red Cross*

The panels of this conference have touched upon a myriad of new technologies, ranging from energy weapons, to drones, robots, satellite technology and space weapons and cyber technology. Some of these technologies are already deployed on today's battlefields, others are still in the realm of science fiction.

The discussions revealed a number of overarching themes, providing food for thought and for further research and thinking. I cannot attempt to summarize all of them, but I would like to highlight five aspects that appeared to be recurring.

Firstly, our discussions revealed a measure of **uncertainty about the facts**. It is not always clear what is technically feasible in today's theatres of war, and less clear what will be feasible in the future and when. It is also not always clear what the humanitarian impact is – of weapons that are already deployed, like drones; that are ready to be deployed, like cyber attacks; or that might be deployed in the future, like autonomous robots. To what extent does this uncertainty hamper our ability to ensure that all new technologies in warfare comply with international humanitarian law? My impression is that while the uncertainty about the specificities and impact of some of these technologies does pose a challenge to applying the law to them, this challenge should not be overstated.

In cyber warfare, for instance, anonymity and interconnectedness of computer networks around the world do indeed seem to pose very serious questions about the way international humanitarian law will play out in the cyber realm. More exchange will need to take place between scientists and lawyers to get clarity on these issues. On the other hand, there seems to be little doubt that cyber attacks are feasible now and can potentially have devastating effects on civilians and civilian infrastructure, for instance by causing the disruption of air control systems, or electricity or water supply systems. Most of us have little or no understanding of how information technology works, and yet there are a number of things we already know and can already say about which effects would be lawful or not should they occur. Most of us do not know how to fly airplanes, but we know about the effects of aerial bombing. In this sense, we should concentrate on the effects of technology we see today in warfare ('in the real world'), and we will probably be able to go a long way in being able to make reasoned statements about the applicability of international humanitarian law and the lawfulness of specific means and methods of warfare in cyber space.

Secondly, the fact that **new technologies remove soldiers further and further away from the battlefield** was a matter of recurring discussion. Many discussants pointed out that remoteness of the soldier to the enemy is nothing fundamentally new. Yet, it is also apparent that a common feature of the new technologies under discussion is that they appear to carry distance one step further – be it by remote-controlled weapons, cyber weapons or robots.

* Also available at: http://www.icrc.org/eng/resources/documents/statement/new-weapon-technologies-statement-2011-09-13.htm

doi:10.1017/S181638311200080X

More thinking is required about the consequences of these remote means and methods of warfare. Firstly, what is the consequence of their use for the definition, the extent of the battlefield? Some have argued that if drones can be flown or cyber attacks launched from anywhere in the world, then anywhere in the world becomes a battlefield. This would in effect be an endorsement of the concept of a 'global battlefield', with the consequence that the use of force rules allowing for incidental civilian loss and damage under the IHL principle of proportionality extend far beyond the scope of what has until now been accepted. This is a notion that the ICRC does not follow.

Long distance means and methods of warfare also pose some questions as to the relationship between, *on the one hand, the use of new technologies to keep soldiers out of harm's way by limiting their exposure to direct combat, and on the other hand their humanitarian impact for the civilian population*. It is probably impossible to say that the remoteness of soldiers from the battlefield will by itself create greater risks for civilians. But given the aversion of many societies and governments to risk the lives of their soldiers, there is a danger that the tendency towards so-called zero casualty wars could lead to choices of weapons that would be dictated by this concern, even if it went to the detriment of the rules of international humanitarian law that protect civilians against the effects of hostilities. Just like high altitude bombing might be safer for soldiers but also in certain circumstances indiscriminate and unlawful, so new technologies, however protective for the troops, will always have to be tested for their compatibility with humanitarian law and in particular their possible indiscriminate or disproportionate effects. This, however, requires that we get a better understanding about the effects of such technologies, in particular their precision and their incidental effects – not only in abstract technological terms but in the way they are concretely being used.

This leads me to a third point, which is a certain **lack of transparency about the effects of certain weapons for the civilian population** – not their potential effect in the future, but the effect of those technologies that are already being used. For instance, there is controversy about the effects of drones: no one appears to know with any measure of certainty the loss of civilian lives, injury to civilians and damage to civilian infrastructure that has been caused by drone attacks. The lack of objective knowledge constitutes a great impediment for the assessment of the lawfulness of weapons or their use in particular circumstances. Transparency in recording the humanitarian consequences of new technologies would certainly be of benefit in this respect – because it would already take into account not only the abstract technical specificities but integrate the actual way in which they are used.

As we heard, however, **new technologies can actually also be tools for more transparency, namely to support the witnessing, recording and investigation of violations**. We heard a very interesting presentation about this in relation to satellite images used by UNITAR to investigate violations during armed conflict. Other technologies come to mind: for instance DNA technology which can sometimes complement traditional forensic science methods, or simple devices such as mobile phone cameras that have been used to record violations. The limits of

using images to illustrate or prove violations in armed conflict, in particular war crimes, is not something new and it is well known that images rarely speak for themselves. But new technologies – together with traditional means, in particular witness accounts – can contribute to uncovering certain violations and this must surely be welcomed.

A fourth recurring theme was that of **responsibility and accountability for the deployment of new technologies**. Whether new technologies will reduce our capacity to allocate responsibility and accountability for violations remains to be seen. As a starting point, it is worth recalling that international humanitarian law parties to conflicts (states and organised armed groups) and international criminal law binds individuals. Just as a number of speakers pointed out, I am not convinced that we have reached the end of accountability with autonomous weapons. Even if artificial intelligence were to be achieved and autonomous systems deployed in armed conflicts, would it not always be the case that any robot is at some point switched on by a human being? If that is the case, then that individual – and the party to the conflict – is responsible for the decision, however remote in time or space the weapon might have been deployed from the moment of the attack. It is a topic that reminds me of Goethe's poem *Der Zauberlehrling* ('the sorcerer apprentice'), who unleashed a broom with destructive artificial intelligence and UAV capacity. Both the apprentice and the magician himself certainly bore their share of responsibility and the magician ultimately had to put his house in order. In cyber space on the other hand, allocation of responsibility does appear to present a legal challenge if anonymity is the rule rather than the exception.

Lastly, the most recurrent overarching theme was maybe that **technology, in itself, is neither good nor bad. It can be a source of good and progress or result in terrible consequences at worst**. This is true most of the time. Transposed to technologies that are weaponised, this means that most weapons are not unlawful as such; whether their use in conflict is lawful or not depends on the circumstances and the way in which they are used.

This being said, some weapons are never lawful and have been banned – blinding laser weapons or landmines, for instance. The same will be true for new technologies: the lawfulness of new means and methods of warfare will usually depend on their use, but it is not excluded that some weapons will be found to be inherently indiscriminate or to cause superfluous injury or suffering, in which case they will have to be banned. This is why the principle reflected in Article 36 of Additional Protocol I that States should verify, when developing new means and methods of warfare, whether their use will be compatible with international humanitarian law is so critical.

If we can draw a lesson from past experience – for instance the deployment of the nuclear bomb – it is that we have trouble anticipating the problems and disasters that we might face in the future. Some say that robots or other new technologies might mean the end of warfare. If robots fight robots in outer space without any impact on human beings other than possible economic loss this would look like the world of knights fighting duels on a meadow outside the city gates, a fairy outcome short of war. But since this is a very unlikely scenario, we have to

focus on the more likely scenario that technologies in armed conflicts will be used to cause harm to the enemy, and that this harm will not be limited to purely military targets but will affect civilians and civilian infrastructure.

So, indeed, let us not be overly afraid about things that might not come – this was the credo of many speakers here in San Remo. But let us nonetheless be vigilant and not miss the opportunity to recall, every time it is needed, that the fundamental rules of international humanitarian law are not simply a flexible moral code. They are binding rules, and so far they are the only legal tool we have to reduce or limit, at least to a small extent, the human cost of war. A multi-disciplinary meeting such as this roundtable is an excellent means to advance towards this goal.

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

SELECTED ARTICLE ON INTERNATIONAL HUMANITARIAN LAW

'Excessive' ambiguity: analysing and refining the proportionality standard

Jason D. Wright*

Jason D. Wright, Esq. is a trained US military lawyer with experience advising on the laws of armed conflict and international human rights law. After serving from 2007 through 2008 as a staff legal adviser and aide-de-camp to a commanding general in Iraq during the height of the multinational counterinsurgency campaign, Mr Wright prepared this article in furtherance of a master of studies in international human rights law from the University of Oxford.

Abstract

This article analyses the jus in bello *proportionality standard under international humanitarian law to assist judge advocates and practitioners in achieving a measure of clarity as to what constitutes 'excessive' collateral damage when planning or executing an attack on a legitimate military objective when incidental harm to civilians is expected. Applying international humanitarian law, the author analyses existing US practice to evidence the need for states to adopt further institutional mechanisms and methodologies to clarify targeting principles and proportionality assessments. A subjective-objective standard for determining 'excessive' collateral damage is proposed, along with a seven-step targeting methodology that is readily applicable to the US, and all other state and non-state actors engaged in the conduct of hostilities.*

* The views reflected herein are those of the author in his personal capacity and do not represent the views or official positions of the US government, US Department of Defense, US Department of the Army, or the US Army's Judge Advocate General's Corps.

doi:10.1017/S1816383113000143

Keywords: proportionality, excessive, collateral damage, civilian casualties, legitimate military objective, incidental harm to civilians.

> The blood of women, children and old people shall not stain your victory. Do not destroy a palm tree, nor burn houses and cornfields with fire, and do not cut any fruitful tree.
>
> The First Caliph, Abu Bakr[1]

In April 2007, the author attended a four-day training course on international humanitarian law (IHL) for US Army judge advocates[2] in preparation for a fifteen-month deployment to Iraq. After a briefing concerning Israel's air strikes in the 2006 Israel-Lebanon War, a panel discussion followed with a senior legal planner from the Israeli military, a legal adviser from the International Committee of the Red Cross (ICRC), and a prominent US humanitarian law commentator. Concerning Additional Protocol I's (API) *jus in bello* proportionality standard,[3] the author asked: 'When weighing the anticipated military advantage against the expected collateral damage, is there any consensus on what is "excessive"?' The answers from the panel varied considerably: from damage that would 'shock the conscience', to 'clearly unreasonable', to just plain 'unreasonable'.

The conceptual confusion offered by these differing opinions led to this current study. Another motivation stemmed from the author's subsequent experience trying to make sense of this confusion during the height of the Iraqi insurgency in 2007 and 2008 as a staff legal adviser to a multinational division headquarters. But most importantly, this question is not some legal nicety that exists in a vacuum. The very lives of civilians hang in this balance. The author has personally seen the human costs of so-called collateral damage and like all legal advisers, practitioners, and commanders, appreciates what is at stake, which is nothing less than the potential life, death, or other sufferings, both unspeakable and untold, of innocents.

For US state practice, there is a great deal of staff coordination in getting this answer right. However, when advising the division headquarters' planning cell and the fire and effects coordination cell on operational and international law issues, the author realized immediately that the legal adviser position required knowledge and expertise on the framework for conducting lawful attacks beyond the existing

1 Reprinted in Dieter Fleck *et al.* (eds), *The Handbook of Humanitarian Law in Armed Conflict*, Oxford University Press, Oxford, 2004, p. 14.

2 Judge advocates are otherwise known as military lawyers. For their role in combat, see Michael F. Lohr and Steve Gallotta, 'Legal support in war: the role of military lawyers', in *Chicago Journal of International Law*, Vol. 4, No. 2, Fall 2003, pp. 465–478.

3 Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (hereinafter API), 8 June 1977, 1125 UNTS 3, Arts. 51(5)(b) and 57(2)(a)(iii) and (b), available at: http://www.unhcr.org/refworld/docid/3ae6b36b4.html (last visited 2 November 2012).

training provided to judge advocates.[4] In short, it became apparent that there were insufficient institutional mechanisms and standards in place despite the good faith efforts by commanders, legal advisers, and staff officers.

Military commanders and staff officers generally want to do what is right – ethically, morally, and legally. For this reason, they demand exacting and sound advice from their legal advisers, who are often in the position of being the first-line defenders of human rights in combat environments. Codified rules of engagement are necessary, but only sufficient when applied subordinate to the overarching conventional and customary legal obligations for the conduct of hostilities.

The intent of this article is to assist state practitioners, as well as other actors engaged in hostilities, providing advice on the legality of planned, lethal attacks under modern IHL. The author examines the current principles and rules relating to the *jus in bello* proportionality standard, and, as an analytical construct, critically assesses US policy as an applicable state practice. Because all states and non-state actors engaged in the conduct of hostilities must comply with international humanitarian law, the principles and institutional framework proposed below may readily assist all states – not just the US. As the seemingly simple question to the panel suggests, the field would benefit from further refinement on the legal considerations for lethal targeting, the *jus in bello* proportionality standard, and practical humanitarian law guidance on protecting civilians from the effects of lawful attacks within the conduct of hostilities – whether international or non-international armed conflict.

This article begins with a brief discussion of the pertinent treaty-based and customary international law standards governing the protections of civilians and civilian objects from attack. Thereafter, US state practice is examined to provide some context for the argument that institutional mechanisms should be in place concerning this critical question about assessing what is 'excessive' collateral damage. The legal development of the proportionality standard is then discussed, and a review of commentaries, scholarly works, and judicial treatment concludes that 'excessiveness' cannot be defined. Notably, there is some academic discord on the applicable standard for its determination – whether subjective to the mind of the commander, an objective 'reasonable commander' approach, or a combination of both. The concluding section then places the debate within the conduct of hostilities – using the US approach as applied to a type of non-international armed conflict, counterinsurgency (COIN) warfare, as the chief example. The article concludes by reconciling the discord, refining the proportionality standard, and framing the question of 'what is excessive collateral damage' within a seven-step targeting methodology.

4 Subject to the commander's guidance and approval, a planning cell develops the campaign plan and specific military operations for the unit (i.e., division) and subordinate units (i.e., brigades), and a fires and effects coordination cell develops the non-lethal and lethal targets sets for approval and appropriate action (e.g., a non-lethal target could be a jobs initiative programme or a disarmament, demobilization, and reintegration initiative).

Protecting civilians from attacks: international humanitarian law obligations and US *opinio juris* examined

> [K]illing of the innocent in war can be licit only when it is done either accidentally or unintentionally (i.e., foreseen but not intended), but even then it is licit only where there is no alternative to it.[5]

API to the Geneva Conventions remains the most authoritative codification of existing customary international law on the protection of civilians during armed conflict. Although the US has not ratified API, it considers most of its provisions to be binding as a matter of customary international law.[6] To protect civilians, API refined the customary concepts of what constitutes a military objective, when civilians lose protection from direct attacks, what type of incidental damage is lawful in an attack, and what precautions planners and commanders must take prior to and during an attack.[7]

Distinction and directing attacks only against legitimate military objectives

The parties to a conflict must distinguish between combatants and civilians, and between military and civilian objects.[8] Belligerents must only direct attacks against legitimate military objectives.[9] Under API, attacks 'mean acts of violence against the adversary, whether in offense or defense'.[10]

There is a two-pronged test for military objectives: (a) does the object, based on its nature, location, purpose, or use, make an effective contribution to the enemy's military action, and (b) does its neutralization present a definite military advantage based on the current circumstances?[11]

An objective analysis of the object's nature, location, current use, or future intended purpose satisfies the first prong.[12] Definite military advantage, on the other hand, involves the commander's subjective determination.[13] This means that the

5 Yuki Tanaka and Marilyn B. Young (eds), *Bombing Civilians: A Twentieth-Century History*, New Press, London, 2009, p. 209.

6 US Department of the Army Judge Advocate Generals Legal Center and School, *Law of War Deskbook*, International and Operational Law Department, Charlottesville, Virginia, 2010, p. 23 (hereinafter LOW DB).

7 Ian Henderson, *The Contemporary Law of Targeting: Military Objectives, Proportionality and Precautions in Attack Under Additional Protocol I*, Martinus Nijhoff, Leiden, 2009, p. 247. For brevity, certain provisions concerning the civilian population are not discussed herein, such as Articles 53 through 56 of API pertaining to, inter alia, special objects (e.g., places of worship, etc.) and the protection of the environment.

8 API, above note 3, Art. 48.

9 API, above note 3, Arts 48 and 52(1); Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *International Committee of the Red Cross, Customary International Humanitarian Law, Vol. 1, Rules*, (hereinafter ICRC Study) Cambridge University Press, Cambridge, 2005, Rule 25, available at: www.icrc.org/. . ./customary-international-humanitarian-law-i-icrc-eng.pdf (last visited 2 November 2012).

10 API, above note 3, Art. 49(1).

11 I. Henderson, above note 7, pp. 51–52; API, above note 3, Art. 52(2); ICRC Study, above note 9, p. 32.

12 I. Henderson, above note 7, pp. 54–60.

13 *Ibid.*, p. 73.

commander must evaluate whether neutralizing this object presents a concrete and direct military benefit to the military interests at stake:

> Even if this system is based to some extent on a subjective evaluation, the interpretation must above all be a question of common sense and good faith for military commanders. In every attack they must carefully weigh up the humanitarian and military interests at stake.[14]

For instance, a missile strike on an enemy tank degrades the enemy's war-fighting capability generally, and depending on where the tank is situated on the battlefield, it might present further concrete and direct tactical advantages were it neutralized. As an example of a state's practice, US policy advances that the military advantage in the prevailing circumstances may be specific to the military objective or cumulative:

> [W]hile the anticipated military advantage must be concrete and direct, it may nonetheless include more than immediate tactical gain from the attack looked at in isolation; it may be calculated in light of other related actions, and it may arise in the future.[15]

However, this approach is not in conformity with the prevailing norm according to the Commentary on the Additional Protocols to the Geneva Conventions:

> The expression 'concrete and direct' was intended to show that the advantage concerned should be substantial and relatively close, and that advantages which are hardly perceptible and those which would only appear in the long term should be disregarded.[16]

Any object that is not a military objective is a civilian object and, as such, is protected from attack.[17]

Civilians, like civilian objects, must receive protection from direct attack.[18] Under conventional law, when there is doubt as to 'whether a person is a civilian, that person shall be considered to be a civilian'.[19] However, as explained below, both combatants and civilians taking a direct part in the hostilities lose protection from direct attack.[20] For international armed conflicts, combatants are inter alia (a) members of the armed forces of a party to the conflict (other than medical personnel and chaplains) or (b) members of militias or other voluntary corps belonging to a party to the conflict, operating under responsible command, having distinctive uniforms, signs, or insignia, carrying their arms openly, and conducting their operations

14 Yves Sandoz, *et al.*, *Commentary on The Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (hereinafter ICRC Commentary), ICRC, Geneva, 17 October 1987, para. 2208, available at: http://www.loc.gov/rr/frd/Military_Law/RC_commentary-1977.html (last visited 2 November 2012).
15 I. Henderson, above note 7, p. 71.
16 ICRC Commentary, above note 14, para. 2209.
17 ICRC Study, above note 9, pp. 26–36.
18 API, above note 3, Art. 51(2).
19 *Ibid.*, Art. 50(1).
20 I. Henderson, above note 7, p. 81.

consistently with the laws and custom of war.[21] Additional Protocol II (APII), which governs non-international armed conflicts, does not use the term combatants, but when referring to belligerents other than state armed forces it refers instead to 'dissident armed forces and other organized armed groups'.[22]

Civilians, as distinct from combatants, are entitled to protection from attack 'unless and for such time as they take a direct part in hostilities'.[23] Such individuals remain classified as civilians, but do become legitimate military targets for the time when they are actively engaged in hostile actions.[24] The ICRC has advanced a three-part test for determining when a civilian takes a direct part in the hostilities, which has likewise been cited by a US Army law of war manual:

a) a harmful act,
b) a direct causal connection between the act and the likely harm resulting from the act, and
c) a belligerent nexus between the act and the support of a party to the conflict.[25]

There are status distinctions for actors in international and non-international armed conflict relative to the protection from direct attack. For international armed conflicts, combatants are legitimate military objectives, and civilians are legitimate military objectives only when, and for such time as, they take a direct part hostilities.[26] For non-international armed conflict these rules apply, but a brief disparity bears mentioning – as the phrase combatants is not used in APII: 'While State armed forces are not considered civilians, practice is not clear as to whether members of armed opposition groups are civilians.'[27] The question arises whether members of armed opposition groups lose protection from attack based generally on continuous membership in such a group or whether some direct hostile act is required:

> To the extent that members of armed opposition groups can be considered civilians . . . [a]pplication of this rule would imply that an attack on members of armed opposition groups is only lawful for 'such time as they take a direct part in hostilities' while an attack on members of governmental armed forces would be lawful at any time. Such imbalance would not exist if members of armed

21 ICRC Study, above note 9, Rules 3 and 4, pp. 11–16; Geneva Convention Relative to the Treatment of Prisoners of War (Third Geneva Convention), 12 August 1949, 75 UNTS 135, Art. 4(A)(3), available at: http://www.unhcr.org/refworld/docid/3ae6b36c8.html (last visited 2 November 2012); API, above note 3, Art. 43(1); I. Henderson, above note 7, pp. 80–81.

22 Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) (hereinafter APII), 8 June 1977, 1125 UNTS 609, Art. 1, available at: http://www.unhcr.org/refworld/docid/3ae6b37f40.html (last visited 2 November 2012); ICRC Study, above note 9, p. 12.

23 API, above note 3, Art. 51(3); ICRC Study, Rule 3, above note 9, pp. 19–24.

24 ICRC Study, Rule 6, above note 9, p. 21.

25 LOW DB, above note 6, pp. 99–100 (citing ICRC, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (2008), available at: http://www.icrc.org/eng/war-and-law/contemporary-challenges-for-ihl/participation-hostilities/index.jsp (last visited 1 November 2012).

26 API, above note 3, Art. 51(3).

27 ICRC Study, above note 9, p. 19 (Rule 5).

> opposition groups were, due to their membership, either considered to be continuously taking a direct part in hostilities or not considered to be civilians.[28]

There is growing support for the proposition that active, continuous membership in an armed opposition group that conducts hostilities may render that fighting civilian a legitimate military objective even when the civilian is not directly participating in a hostile act.[29]

Distinction and avoiding indiscriminate attacks

The fundamental principle of distinction also prohibits indiscriminate attacks, 'attacks of a nature to strike military objectives and protected persons and objects without distinction'.[30] API defines indiscriminate attacks as those which:

> [a] 'are not directed at a specific military objective . . .; [b] employ a method or means of combat which cannot be directed at a specific military objective'; or . . . [c] whose effects 'are of a nature to strike military objectives and civilians and civilian objections without distinction'.[31]

For lethal targeting, belligerents must take reasonable care in executing the attack to ensure that only the military objective is attacked.[32] The essential elements of this conventional obligation include positively identifying the military objective, directing the method of attack to that target, and ensuring that the weapon hits the target 'with some degree of likelihood'.[33] Examples of indiscriminate attacks include firing blindly, randomly releasing bombs without positive target identification, and firing imprecise missiles at military objectives that are co-located with civilians or civilian objects.[34] For example, consistent with these obligations, coalition aircrews in the Gulf War were properly 'directed not to expend their munitions if they lacked positive identification of their targets'.[35] For APII governing non-international armed conflicts, there is no express treaty recognition of the obligation to avoid indiscriminate attacks similar to Articles 51 and 57 of API, but Article 13(2)'s requirement that the civilian population 'shall not be the object of attack' embraces the duty to avoid indiscriminate attacks.[36]

28 *Ibid.*, 21 (Rule 6).
29 I. Henderson, above note 7, pp. 95–97. For a concise discussion, see Program on Humanitarian Policy and Conflict Resolution, *Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare*, Harvard University Press, Cambridge, MA, 2009, pp. 117–124 available at: http://www.ihlresearch.org/amw/manual/ (last visited 1 November 2012) (hereinafter HPCR Commentary).
30 Nils Melzer, *Targeted Killing in International Law*, Oxford University Press, Oxford, 2009, p. 355.
31 API, above note 3, Arts 51(4)–(5)(a); ICRC Study, above note 9, pp. 37–50.
32 A. P. V. Rogers, *Law on the Battlefield*, Manchester University Press, Manchester, 2004, p. 23.
33 *Ibid.*, p. 24.
34 Yoram Dinstein, *The Conduct of Hostilities Under the Law of International Armed Conflict*, Cambridge University Press, Cambridge, 2004, p. 118.
35 US Department of Defense, *Report to Congress: Conduct of the Persian Gulf War* (hereinafter DoD Report), Pentagon, Washington, D.C., 1992, p. 698, available at: www.ndu.edu/library/epubs/cpgw.pdf (last visited 2 November 2012).
36 ICRC Study, above note 9, pp. 38–39 (per Rule 11 '[n]o official contrary practice was found with respect to either international or non-international armed conflicts').

Proportionality in attack

'Proportionality' as a term transcends international law and has a specific meaning depending on its reference in international law, IHL, or international human rights law. Proportionality refers generally to four distinct concepts: (a) the requirement of proportionate force under the *jus ad bellum* relating to a state's resort to the use of force in self-defence under Article 51 of the UN Charter; (b) the concept of a proportionate, belligerent response in reprisal against an adversary's violation of IHL; (c) the *jus in bello* obligation to ensure that an attack does not cause disproportionate collateral damage;[37] and (d) a state's duty under international human rights law to ensure that the use of lethal force for law enforcement purposes is restrained and in proportion to the harm presented: '[w]henever the lawful use of force and firearms is unavoidable, law enforcement officials shall . . . [e]xercise restraint in such use and act in proportion to the seriousness of the offence and the legitimate objective to be achieved.'[38]

A discussion of the philosophical origins of this transcendental concept of proportionality and its intersections between international human rights law and IHL is beyond the scope of this article.[39] Proportionality in attack within the conduct of hostilities is discussed in greater detail below.

Precautions in attack

Conventional and customary IHL obligates the attacking party to take sufficient precautions prior to an attack.[40] API codifies the current conventional and customary international law provisions relating to the necessary precautions in an attack. It specifies that 'constant care shall be taken to spare the civilian population, civilians and civilian objects'.[41] Pursuant to this affirmative duty, those who plan and approve attacks must:

a) verify military objectives. Do 'everything feasible to verify' that the target is a military objective, and not civilians, civilian objects, or other protected persons or places;
b) avoid or minimize collateral damage. 'Take all feasible precautions' in choosing both the 'means and methods of attack' with a 'view to avoiding, and in any event minimizing, incidental loss or civilian life, injury to civilians and damage to civilian objects'; and

37 API, above note 3, Art. 51(5)(b); ICRC Study, Rule 14, above note 9, pp. 46–50. I. Henderson, above note 7, pp. 180–181; A. P. V. Rogers, above note 32, p. 17.
38 Basic Principles on the Use of Force and Firearms by Law Enforcement Officials, 7 September 1990, Principle 5, available at: http://www2.ohchr.org/english/law/firearms.htm (last visited 1 November 2012).
39 For an excellent examination of the lawfulness of state-sponsored targeted killings under international human rights law (i.e., the law enforcement paradigm) and international humanitarian law (i.e., the conduct of hostilities paradigm), see generally N. Melzer, above note 30.
40 API, above note 3, Art. 57; ICRC Study, above note 9, pp. 51–67; Hague Convention IV, Respecting the Laws and Customs of War on Land, 18 October 1907, 36 Stat. 2277, Art. 2(3) (hereinafter Hague IV).
41 API, above note 3, Art. 57(1).

c) refrain from excessive collateral damage. 'Refrain from deciding to launch an attack which may be expected to cause' collateral damage 'which would be excessive' relative to the 'concrete and direct military advantage anticipated'.[42]

Although current US Army legal doctrine fails to direct critical attention to such precautions, the Army's 1956 Law of Land Warfare guide obligates the planners of an attack to verify the military objective reasonably prior to an attack, to avoid attacks creating 'probable losses in lives and damage to property disproportionate to the military advantage anticipated', and to provide warnings prior to a bombardment to facilitate the evacuation of civilians from the impact area.[43] Generally, feasibility determinations depend on multiple factors, such as the availability of intelligence concerning the target and target area, availability of weapons, assets, and different means of attack, level of control over the territory to be attacked, urgency of attack, and 'additional security risks which precautionary measures may entail for the attacking forces or the civilian population'.[44]

This obligation to minimize collateral damage in planning the attack precedes the subsequent obligation to refrain from disproportionate attacks: 'In other words, there is a requirement to minimize collateral damage and not merely to cause no more than proportional collateral damage.'[45] For instance, even when choosing a plan of attack that minimizes collateral damage, planners must still refrain from the attack if the expected collateral damage would be excessive to the military advantage anticipated.

Planners, commanders, operators who execute an attack, and anyone who exercises effective control over the attack must cancel or suspend it if 'it becomes apparent' that: (a) the object is no longer a military objective, (b) the object is subject to special protection, or (c) the expected collateral damage would be excessive relative to the anticipated military advantage.[46]

For attacks affecting the civilian population, planners and operators must give 'effective advance warning' unless the circumstances do not permit, such as assaults necessitating surprise.[47] Planners have a duty to consider and comply with the notice requirement where some harm to civilians or civilian objects is anticipated. There can be no general policy of not giving advance warning of attacks because the circumstances of each attack must be considered.[48] Where the

42 API, above note 3, Art. 57(2)(a)(iii); ICRC Study, above note 9, pp. 51–61.
43 Compare US Department of the Army Judge Advocate Generals Legal Center and School, *Operational Law Handbook*, International and Operational Law Department, Charlottesville, VA, 2009, pp. 10–13 (hereinafter OPLAW HB) with US Department of the Army Field Manual 27–10, *The Law of Land Warfare*, Pentagon, Washington, D.C., 15 July 1976, Rules 41–44, available at: http://www.afsc.army.mil/gc/files/fm27-10.pdf (last visited 2 November 2012).
44 N. Melzer, above note 30, p. 365.
45 I. Henderson, above note 7, p. 168.
46 API, above note 3, Art. 57(2)(b); ICRC Study, above note 9, pp. 60–62; I. Henderson, above note 7, p. 235.
47 API, above note 3, Art. 57(2)(c); ICRC Study, above note 9, pp. 62–65.
48 I. Henderson, above note 7, p. 187; Waldemar A. Solf, 'Protection of civilians against the effects of hostilities under customary international law and Protocol 1', in *American Journal of International Law and Policy*, Vol. 80, No. 1, January 1986, p. 132.

circumstances do not permit effective advance warning, such as those that do require surprise in the attack, a commander should take other measures to ensure that civilians have a chance to protect themselves. On this point, the ICRC Commentary to API illustrates that providing a warning of a missile strike 'may be inconvenient when the element of surprise in the attack is a condition of success'; however, civilians must still be on notice as to the types of facilities, objects, or objectives that are likely to be subject to attack.[49]

Finally, there is a 'lesser of two evils' rule.[50] Where there is a choice among different military objectives for obtaining a 'similar military advantage', commanders must attack that objective 'which may be expected to cause the least danger to civilian lives and civilian objects'.[51]

To establish a baseline of understanding, the foregoing has provided a brief restatement of the IHL principles that govern targeting and the protection of the civilian population. A critical examination of US doctrine and policy on targeting follows to evidence just one state's practice for the purposes of exposing the difficulties of determining what constitutes 'excessive' collateral damage.

A state practice examined: US expressions of IHL doctrine

From personal experiences, both in US-sponsored training opportunities, multiple war game exercises, and real-life situations in Iraq as a lawyer advising on IHL, the author found that US practice almost exclusively relies on its own rules of engagement (ROE) when making targeting and proportionality assessments.[52] Rarely were legal advisers directed or encouraged in their training to apply the governing standards under conventional or customary IHL before examining whether a particular course of action was consistent with any controlling rules of engagement. This shortcoming, in many respects, is likely due to the cursory nature of the explanations of IHL provisions that are provided to new judge advocates during initial training and pre-deployment training, and to the under reliance on the treaty provisions in authoritative, US law of war manuals. In short, the author determined that ROE were necessary, but far from sufficient. The following highlights the US view on the governing IHL provisions, and then discusses ROE and targeting doctrine in greater detail.

The US Department of Defense (DoD) obligates its service components (that is, the Army, Navy, Air Force, and Marines) and service members to comply with the laws of war during all military operations and armed conflicts.[53] Per DoD policy, the law of war comprises the international legal standards

49 ICRC Commentary, above note 14, paras. 2223–2225.
50 *Ibid.*, para. 2226.
51 API, above note 3, Art. 57(3); ICRC Study, above note 9, pp. 65–67.
52 The US practice of developing and applying ROE is discussed in greater detail below.
53 US Department of Defense, Directive 2311.01E, *DoD Law of War Program*, Pentagon, Washington, D.C., 9 May 2006, p. 2, available at: http://www.dtic.mil/whs/directives/corres/pdf/231101e.pdf (last visited 2 November 2012).

regulating the conduct of hostilities and all binding treaties and applicable customary international law.[54]

As contended, training modules and doctrine would be much improved if judge advocates were trained to refer to the primary, authoritative sources, such as the Geneva Conventions and its Additional Protocols, prior to examining whether a course of action complies with the ROE. The following captures the US doctrinal attempts to address conventional and customary obligations for practitioners.

Current doctrine from the US Army's accredited Judge Advocate General's (JAGC) Legal Center and School[55] emphasizes the following fundamental elements of the laws of war for military lawyers to consider: military necessity, distinction, proportionality, and no unnecessary suffering.[56] Army lawyers are instructed to address these elements in all circumstances and to follow specific international legal obligations, such as 'treaties and international agreements to which the United States is a party, and applicable customary international law'.[57]

Military necessity as codified in Article 23 of the Hague Regulation of 1907 and expressed in doctrine allows the destruction and seizure of the enemy's property where 'such destruction or seizure be imperatively demanded by the necessities of war'.[58] The principle of military necessity, while allowing the use of lethal force, 'does not authorize acts otherwise prohibited by the [laws of war]'.[59] Prohibited acts include the intentional targeting of protected persons or objects, such as civilians taking no direct part in the hostilities.[60]

The element of distinction, qualified by doctrine as the principle of discrimination, requires that combatants and military objectives be distinguished from civilians and civilian objects; accordingly, 'parties to a conflict must direct their operations only against combatants and military objectives'.[61] Doctrine does incorporate API's definition of military objectives.[62] When a belligerent commits an indiscriminate attack in violation of customary international law and API, its actions violate this principle of distinction.[63]

Current Army doctrine indicates that the proportionality principle is not a separate legal requirement, but fundamentally a balancing test between the principles of military necessity and 'unnecessary suffering in circumstances when an attack may cause incidental damage to civilian personnel or property'.[64] Since 1956,

54 *Ibid.*
55 This institution provides legal training to judge advocates and develops legal doctrine. See https://www.jagcnet.army.mil (last visited 1 November 2012).
56 OPLAW HB, above note 43, pp. 10–13.
57 *Ibid.*, p. 10.
58 *Ibid.*, p. 10, citing Hague Convention IV, above note 40, Art. 23.
59 *Ibid.*, at 10.
60 *Ibid.*, at 11.
61 *Ibid.*
62 *Ibid.*, p. 12 (defined as 'objects which by their nature, location, purpose or use, make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage').
63 *Ibid.*
64 *Ibid.*

and updated in 1976, the Army's law of war compendium has included a specific proportionality formula in relation to lawful attacks:

> loss of life and damage to property incidental to attacks must not be excessive in relation to the concrete and direct military advantage expected to be gained. Those who plan or decide upon an attack, therefore, must take all reasonable steps to ensure not only that the objectives are identified as military objectives . . . but also that these objectives may be attacked without probable losses in lives and damage to property disproportionate to the military advantage anticipated.[65]

Recent doctrine changes the terminology from 'probable losses' to the 'anticipated' harm.[66] Incidental damage is defined as lawful when 'unavoidable and unintentional damage to civilian personnel and property incurred while attacking a military objective'.[67] A 'military advantage' may constitute a specific tactical or (controversially as discussed below) overall strategic gain.[68] Per doctrine, there is no clarification or guidance as to what constitutes 'excessive' damage. While doctrine notes that proportionality balancing involves a 'variety' of considerations, it fails to outline such considerations with any particularity:

> Balancing . . . may be done on a target-by-target basis but also . . . in an overall sense against campaign objectives . . . [p]roportionality balancing typically involves a variety of considerations, including the security of the attacking force.[69]

Finally, the principle of minimizing unnecessary suffering applies to combatants, and as codified in the early twentieth century, expressly forbids the use of 'arms, projectiles or material calculated to cause unnecessary suffering'.[70] Otherwise construed as a principle stemming from the requirements of humanity, no generally agreed-upon definition of this principle exists, but the US applies it when reviewing the legal uses of weapons.[71]

A state practice examined: US legal considerations in targeting

The DoD regulates the use of force by its components and members through classified standing ROE.[72] ROE are '[d]irectives issued by competent military

65 Land Warfare, above note 43, Rule 41 (citing the 1956 rules which provide that 'loss of life and damage to property must not be out of proportion to the military advantage to be gained').
66 OPLAW HB, above note 43, p. 12.
67 *Ibid.*
68 *Ibid.*
69 *Ibid.*
70 *Ibid.*, p. 12, citing Hague IV, above note 40, Art. 23(e).
71 *Ibid.*
72 US Chairman of the Joint Chiefs of Staff, Instruction 3121.01B, *Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces*, Pentagon, Washington, D.C., 13 June 2005 (unclassified portion reprinted in OPLAW HB, above note 43, pp. 82–96).

authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces'.[73]

Subordinate commanders ensure that the DoD's standing ROE are promulgated to their units and members, and may generate additional, more restrictive, mission-specific ROE for their operational environment.[74] These standing and mission-specific ROE derive from conventional and customary international law principles and may contain constraints based on policy objectives, mission requirements, US domestic law, and host-nation law.[75]

Targeting is defined as the 'process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities'.[76] Per doctrine, all targeting decisions involving attacks must comply with controlling ROE and IHL to include the 'fundamental principles of military necessity, unnecessary suffering, proportionality, and distinction (discrimination)'.[77]

Targeting doctrine warns planners that, in relation to avoiding collateral damage, the primary threats to the civilian population depend on 'engagement techniques, weapon used, nature of conflict, commingling of civilian and military objects, and armed resistance encountered'.[78] Planners should further verify with sound intelligence that attacks are directed only against military targets and that any incidental 'civilian injury or collateral damage to civilian objects must not be excessive in relation to the concrete and direct military advantage expected to be gained'.[79] Additionally, when the circumstances permit, advance warning of the attack should be given to allow civilians to depart the targeted area.[80] Finally, doctrine provides that the attack must be cancelled or suspended when 'it becomes apparent that a target is no longer a lawful military objective'.[81]

To assist planners and commanders, classified DoD methodology on the targeting process – to include a method for assessing collateral damage – is contained in a companion regulation to the DoD's standing ROE entitled Joint Methodology for Estimating Collateral Damage for Conventional Weapons, Precision, Unguided, and Cluster.[82] Beyond this controlling regulation, mission-specific ROE likewise may contain specific constraints on planning and executing

73 US Department of Defense, Joint Publication 1-02, *Dictionary of Military and Associated Terms* (hereinafter DoD Terms), Pentagon, Washington, D.C., 15 August 2012, p. 473, available at: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (last visited 2 November 2012).
74 OPLAW HB, above note 43, p. 83.
75 *Ibid.* , pp. 73–74.
76 DoD Terms, above note 73, p. 538.
77 US Department of Defense, Joint Publication 3-60, *Joint Targeting* (hereinafter Joint Targeting), Pentagon, Washington, D.C., 12 April 2007, pp. E1-2, available at: www.aclu.org/files/dronefoia/dod/drone_-dod_jp3_60.pdf (last visited 2 November 2012).
78 *Ibid.*, p. E-4.
79 *Ibid.*
80 *Ibid.*
81 *Ibid.*
82 *Ibid.*, p. G-1 (citing US Chairman of the Joint Chiefs of Staff, Manual 3160.01A, *Joint Methodology for Estimating Collateral Damage for Conventional Weapons, Precision, Unguided, and Cluster* (classified publication).

lawful attacks based on IHL, policy and mission objectives, host-nation requirements, and other military considerations.[83]

The classified joint methodology codifies standards for estimating the expected collateral damage in an attack, provides means and recommendations to mitigate any expected damage, and assists commanders with 'weighing collateral risk against military necessity and assessing proportionality within the framework of the military decision-making process'.[84] The classified collateral damage estimate (CDE) methodology consists of a five-step process, summarized in an unclassified format as follows:

> As the methodology . . . moves through the CDE levels, the level of analysis and risk the commander accepts increases.
>
> CDE 1 determines whether the target can be positively identified and is a valid military target. CDE 1 also provides an initial collateral damage estimate for the employment of all conventional munitions . . .
>
> CDE 2 provides an estimate for precision-guided unitary and cluster munitions based on nominal weaponeering restrictions. CDE 2 also provides an assessment of whether a target meets the minimum requirements for employment of air-to-surface and surface-to-surface unguided munitions . . .
>
> CDE 3 provides specific [effective miss distance] values and weaponeering assessments for all precision and unguided munitions to ensure the desired effect is achieved while mitigating collateral damage . . .
>
> CDE 4 further refines the CDE 3 assessment by incorporating collateral structure type with the goal of achieving a low CDE while minimizing tactical restrictions . . .
>
> CDE 5, casualty estimation, is employed when some level of collateral damage is unavoidable.[85]

This five-step CDE process begins at target development and continues until the execution of the attack.[86] Planners use the CDE methodology for deliberate targets, that is, targets that have been planned for future execution.[87] Deliberate targeting is subject to a staff process with input from many stakeholders beyond the legal adviser. It involves coordinating historical and real-time intelligence, weaponeering, and logistical constraints, and the planning horizon is dependent on the battlefield circumstances that are ruling at the time.

83 See, e.g., US Department of the Army, Field Manual 3-24, *Counterinsurgency* (hereinafter COIN Manual), Pentagon, Washington, D.C., 15 December 2006, p. D-2, available at: www.fas.org/irp/doddir/army/fm3-24.pdf (last visited 2 November 2012).

84 Joint Targeting, above note 77, p. G-1.

85 *Ibid.*; see also US Department of Defense, *Joint Fires and Targeting Handbook* (hereinafter Targeting HB), Pentagon, Washington, D.C., 19 October 2007, pp. III-77–78, available at: http://www.dtic.mil/doctrine/doctrine/jwfc_pam.htm (last visited 2 November 2012).

86 Joint Targeting, above note 77, p. II-10.

87 *Ibid.*, p. I-6.

Dynamic targeting, conversely, 'prosecutes targets of opportunity and changes to planned targets or objectives'.[88] For planning and assessing the legality of planned strikes by aircraft or artillery this CDE methodology assists staff officers and commanders in complying with IHL and applicable ROE to minimize expected harm to civilians.[89]

In conclusion, conventional and customary international law must be the starting point in any targeting analysis and proportionality assessment. US Army legal doctrine does provide that the legality of any attack under the *jus in bello* must satisfy fundamental principles of the laws of war, such as those of military necessity, distinction, proportionality, and humanity (that is, no unnecessary suffering). Additional guidance related to the protection of the civilian population when targeting military objectives and estimating collateral damage is provided to practitioners by DoD doctrine; however, there remains ambiguity as to the application of the *jus in bello* proportionality standard.[90]

The five-step collateral damage estimate methodology provides a useful institutional mechanism, but it fails to answer what constitutes excessive collateral damage and otherwise does not incorporate a fully integrated targeting analysis that applies IHL in the first instance. Considering conventional and customary IHL and US doctrine as a model of a particular state's practice, legal advisers and other practitioners are still left with the central question concerning collateral damage – what is excessive?

Deconstructing the *jus in bello* proportionality standard

> 'Wilt thou also destroy the righteous with the wicked? . . . [If] there be fifty righteous within the city: wilt thou also destroy and not spare the place for the fifty righteous that are therein?' . . . 'I will not destroy it for ten's sake.'
>
> Abraham and the Lord[91]

The *jus in bello* proportionality standard is a conventional and customary law standard that prohibits attacks where the expected incidental loss of civilian life, injury to civilians or damage to civilian objects would be excessive in relation to the concrete and direct military advantage anticipated.[92] Intentionally causing an attack with the knowledge that it will result in excessive collateral damage in comparison to the anticipated military advantage is a grave breach of API when causing death or

88 *Ibid.*, p. I-7. For classification reasons, dynamic or hasty targeting is not discussed herein, but the legal obligations remain unchanged.

89 Joint Targeting, above note 77, p. E-3; Targeting HB, above note 85, p. III-77.

90 For additional doctrine, please see US Army Tactics, Techniques, and Procedures, *Civilian Casualty Mitigation*, Pentagon, Washington, D.C., 18 July 2012, available at: http://www.fas.org/irp/doddir/army/attp3-37-31.pdf (last visited 2 November 2012). (The pamphlet emphasizes the need to mitigate civilian casualties in all combat actions and in all combat environments. It adds little to the targeting matters discussed herein, but the general expressions of US Army policy may prove useful for practitioners seeking to evaluate US state practice.)

91 The Holy Bible, Genesis, 18:20–33.

92 API, above note 3, Arts. 51(5)(b) and 57(2)(a)(iii) and (b).

serious injury to body or health.[93] The International Criminal Court (ICC) also has subject matter jurisdiction for States Party to the Rome Statute where such damage is 'clearly' excessive in relation to the concrete and direct 'overall' military advantage anticipated.[94]

With respect to targeting, 'the fundamental issue remains that it is difficult to determine exactly what is excessive in any given case'.[95] The following analysis presents a brief historical backdrop for the *jus in bello* proportionality standard and as an example of a state practice, the US' modern treaty recognition. The article then considers both interpretative commentaries and judicial treatment of the standard.

Historical development: from the Lieber Code to customary international law

The origins of the proportionality standard in the conduct of hostilities can be traced to US Army's Lieber Code of 1863.[96] In embracing the principle of military necessity, the Lieber Code implies that incidental and unavoidable collateral damage is permissible subject to military exigencies.[97]

The St. Petersburg Declaration of 1868 further embraces the principle of military necessity and declares that the only purpose of war should be to 'weaken the military forces of the enemy'.[98] The Hague Regulation IV of 1907 similarly codifies this principle: 'it is especially forbidden . . . [t]o destroy or seize the enemy's property, unless such destruction or seizure be imperatively demanded by the necessities of war'.[99] A logical deduction from the principle of military necessity, therefore, is the obligation to observe the requirements of humanity, such as minimizing collateral damage to the greatest extent possible.[100]

Following the first systematic use of aerial warfare as a means of attack during World War I, a commission of jurists drafted the 'Rules of Air Warfare' from 1922 to 1923.[101] Although never formally adopted, these rules signal the developing

93 API, above note 3, Art. 85(3)(b) and (c).

94 Rome Statute of the International Criminal Court (last amended 2010) (hereinafter Rome Statute), 17 July 1998, 2187 UNTS 90, Art. 8(2)(b)(iv), available at: http://www.unhcr.org/refworld/docid/3ae6b3a84.html (last visited 2 November 2012).

95 I. Henderson, above note 7, p. 247.

96 William J. Fenrick, 'The rule of proportionality and Protocol I in conventional warfare', in *Military Law Review*, Vol. 98, No. 1, Fall 1982, p. 95; A. P. V. Rogers, above note 32, p. 17.

97 *Instructions for the Government of Armies of the United States in the Field*, General Orders No. 100, 24 April 1863, Arts 15 and 22, available at: http://www.loc.gov/rr/frd/Military_Law/pdf/Instructions-gov-armies.pdf (last visited 2 November 2012). Compare [Article 15] 'Military necessity admits of all direct destruction of life or limb of armed enemies, and of other persons whose destruction is incidentally unavoidable in the armed contests of the war' with [Article 22] 'Nevertheless, as civilization has advanced during the last centuries . . . [t]he principle has been more and more acknowledged that the unarmed citizen is to be spared in person, property, and honor as much as the exigencies of war will admit'.

98 *Declaration Renouncing the Use, in Time of War, of Explosive Projectiles under 400 Grammes Weight*, 138 Consol. TS 297, 11 December 1868, available at: http://www.icrc.org/IHL.NSF/ (last visited 2 November 2012).

99 Hague IV, above note 40, Art. 23.

100 W. F. Fenrick, above note 96, p. 96; N. Melzer, above note 30, pp. 357–358.

101 Y. Tanaka and M. B Young, above note 5, p. 78.

tension between military necessity and the protection of the civilian population during air attacks. In particular, Article 24 bans air attacks on military objectives within populated areas where 'an undiscriminating bombardment of the civil population would result therefrom'.[102] This article signifies the initial development of the modern *jus in bello* proportionality standard:

> [Within populated areas, bombardments of military objectives is legitimate] 'provided there is a reasonable presumption that the military concentration is important enough to justify the bombardment, taking into account the danger to which the civil population will thus be exposed'.[103]

In 1956, following the high non-combatant casualty rates in World War II due to strategic area bombing, the ICRC attempted to advance the protection of civilians in war by presenting the 'Draft Rules for the Limitation of the Dangers Incurred by the Civilian Population in Time of War'.[104] The Draft Rules, which were never formally adopted, oblige commanders to refrain from launching an attack where the collateral damage would be 'disproportionate to the military advantage anticipated':

> The person responsible for ordering or launching an attack shall . . . take into account the loss and destruction which the attack . . . is liable to inflict upon the civilian population. He is required to refrain from the attack if, after due consideration, it is apparent that the loss and destruction would be disproportionate to the military advantage anticipated.[105]

Under the Draft Rules, those who execute the attack must minimize the damage to the civilian population in carrying out the attack and suspend it if necessary.[106]

The development of the principle of proportionality led to API, the first treaty that attempts to define for international armed conflict 'what level of incidental damage is lawful when conducting an attack, and what other precautions must be taken when conducting an attack'.[107]

For non-international armed conflicts, APII does not specifically reference a proportionality standard similar to Articles 51 and 57 of API, but its preamble recognizes that 'the human person remains under the protection of the principles of humanity and the dictates of the public conscience', and Article 13(2) stresses that 'the civilian population as such, as well as individual civilians, shall not be the object of attack'.[108] Consequently, there appears to be no question that the *jus in bello* principle of proportionality is applicable to both international and

102 *Rules for Air Warfare Drafted by a Commission of Jurist at The Hague*, December 1922 to February 1923, Art. 24(3) available at: http://www.icrc.org/ihl/INTRO/275?OpenDocument (last visited 2 November 2012).
103 *Ibid.*, Art. 24(4).
104 *Draft Rules for the Limitation of the Dangers Incurred by the Civilian Population in Time of War*, 1956, available at: http://www.icrc.org/ihl/INTRO/420?OpenDocument (last visited 2 November 2012).
105 *Ibid.*, Art. 8.
106 *Ibid.*, Art. 9.
107 I. Henderson, above note 7, p. 247.
108 APII, above note 22, preamble and Art. 13(2).

non-international armed conflict and that it is a rule of customary international law.[109]

US recognition and other treaty provisions

As previously stated, the US, which has signed but not ratified API, considers most of its provisions, including the *jus in bello* proportionality principle, to be authoritative of customary IHL.[110] Aside from attaining status as a customary norm, a proportionality criminal standard has been incorporated in Article 8(2)(b)(iv) of the Rome Statute for the International Criminal Court (discussed in greater detail below).[111] As discussed above, API likewise criminalizes violations of the proportionality standard when committed wilfully in the knowledge that the attack would cause excessive collateral damage.[112]

Subject to reservations and declarations, the US has ratified the 1980 Certain Conventional Weapons (CCW) Treaty and its subsequent Protocols.[113] In 1995 the US ratified Protocol II to CCW, which contains a proportionality standard with terminology identical to Articles 51 and 57 of API.[114] In 1999 the US ratified Amended Protocol II, which also included the proportionality standard without change.[115] However, Article 3(10) of Amended Protocol II in relation to precautionary measures does modify the temporal element tactically where, for the use of mines, planners must consider both the short- and long-term military requirements and short- and long-term effects on the civilian population.[116]

109 ICRC Study, above note 9, Rule 14 p. 46 ('Launching an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and directly military advantage anticipated, is prohibited').

110 DoD Report, above note 35, p. 691. For recognition of US practice, see LOW DB, above note 6, pp. 142–143; DoD Report, above note 35, pp. 697–698 ('The principle of proportionality acknowledges the unfortunate inevitability of collateral civilian casualties and collateral damage to civilian objects when non-combatants and civilian objects are mingled with combatants and targets, even with reasonable efforts by the parties to a conflict to minimize collateral injury and damage').

111 ICRC Study, above note 9, pp. 49–50.

112 API, above note 3, Art. 85.

113 Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (hereinafter CCW), 19 ILM 1523, 10 October 1980, available at: http://www.icrc.org/eng/resources/documents/publication/p0811.htm (last visited 2 November 2012).

114 Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices (Protocol II to CCW), 10 October 1980, Art. 3(3), available at: http://www.icrc.org/IHL.NSF/ (last visited 2 November 2012).

115 Protocol II to CCW, as amended 3 May 1996, Art. 3(8)(c), available at: http://www.icrc.org/IHL.NSF/ (last visited 2 November 2012) ('Indiscriminate use is any placement of such weapons … which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated').

116 *Ibid.*

Modern commentaries

In 1987 the ICRC published a *Commentary* to API that summarizes and analyses the drafting history of the Protocols.[117] During the Protocols' negotiations, states significantly disagreed on both the terminology and formula for the proportionality standard.[118] This disagreement derived from the 'delicate problem' of specifically comparing the dissimilar values of collateral damage and military advantage in an attack and, from a broader perspective, generally balancing humanitarian and military interests in the conduct of hostilities.[119]

For the application of the standard, the ICRC analysis suggests, to some extent, a subjective standard as it 'allows for a fairly broad margin of judgement' to commanders.[120] Although a 'subjective evaluation', commanders must still exercise common sense and good faith in weighing the humanitarian and military values for an attack.[121] With respect to determining what is 'excessive', the *ICRC Commentary* asserts that API 'does not provide any justification for attacks which cause extensive civilian losses and damages', irrespective of a comparative anticipated military advantage.[122]

The 2005 ICRC customary law study offers state summaries on 'Determination of the Anticipated military advantage' and 'Information Required for Judging Proportionality in Attack',[123] but the analysis does not present a direct rule or standard for determining what amounts to excessive collateral damage.

In March 2010 the Program on Humanitarian Policy and Conflict Research (HPCR) at Harvard University, in collaboration with a group of humanitarian law experts, approached this issue.[124] The experts, at variance with the ICRC's commentary subjective characterization of the standard, declared the standard for proportionality to be 'objective in that the expectations must be reasonable . . . "expected" collateral damage and "anticipated" military advantage, for these purposes, mean that that outcome is probable, i.e. more likely than not'.[125] Concerning the conceptual confusion regarding 'excessive', the experts write:

> The term 'excessive' is often misinterpreted. It is not a matter of counting civilian casualties and comparing them to the number of enemy combatants that have been put out of action. It applies when there is a significant imbalance between the military advantage anticipated . . . and the expected collateral damage to civilians and civilian objects.[126]

117 ICRC Commentary, above note 14.
118 *Ibid.*, p. 624, para. 1979.
119 *Ibid.*, p. 624, para. 1979 and pp. 683–684, para. 2208.
120 *Ibid.*, pp. 683–684, paras. 2208–2210.
121 *Ibid.*
122 *Ibid.*, p. 626, para. 1980.
123 ICRC Study, above note 9, Vol. II, Practice Relating to Rule 14.
124 HPCR Commentary, above note 29. See also HPCR, *Manual on International Law Applicable to Air and Missile Warfare*, 15 May 2009, available at: http://www.ihlresearch.org/amw/manual/ (last visited 2 November 2012).
125 HPCR Commentary, above note 29, pp. 91–92.
126 *Ibid.*, p. 92.

Turning to the application of the proportionality test, the experts suggest a scaled approach, with qualifiers such as marginal, substantial, and high:

> The fact that collateral damage is extensive does not necessarily render it excessive. The concept of excessiveness is not an absolute one. Excessiveness is always measured in light of the military advantage that the attacker anticipates to attain through the attack. If the military advantage anticipated is marginal, the collateral damage expected need not be substantial in order to be excessive. Conversely, extensive collateral damage may be legally justified by the military value of the target struck, because of the high military advantage anticipated by the attack.[127]

Accordingly, the HPCR experts disagree with the ICRC's assertion that 'extensive' collateral damage is prohibited in all circumstances.[128] The HPCR experts could not agree as to whether an attack's indirect effects on the civilian population must be included in the collateral damage assessment, an issue relevant to the potential suffering of a civilian population.[129] However, there is agreement that remote or unforeseen indirect effects should not be factored in.[130] Although beyond the scope of this article, it bears mentioning that this debate is now squarely at issue with the US's increased used of drone attacks in Pakistan and elsewhere – what about psychological suffering especially when it is no longer remote or unforeseen?

> US drone strike policies cause considerable and under-accounted for harm to the daily lives of ordinary civilians, beyond death and physical injury. Drones hover twenty-four hours a day over communities in northwest Pakistan, striking homes, vehicles, and public spaces without warning. Their presence terrorizes men, women, and children, giving rise to anxiety and psychological trauma among civilian communities. Those living under drones have to face the constant worry that a deadly strike may be fired at any moment, and the knowledge that they are powerless to protect themselves. These fears have affected behavior.[131]

Finally, the HPCR experts conclude that national or policy constraints (for example, ROE) that require authorization at certain levels of command when collateral damage reaches a pre-determined threshold do not obviate the requirement to conduct a proportionality assessment or otherwise make the attack lawful.[132]

127 *Ibid.*
128 *Ibid.*
129 *Ibid.*, p. 91.
130 *Ibid.*
131 International Human Rights and Conflict Resolution Clinic (Stanford Law School) and Global Justice Clinic (NYU School of Law), *Living under Drones: Death, Injury, and Trauma to Civilians from US Drone Practices in Pakistan*, September 2006, pg. vii, available at: http://livingunderdrones.org/report/ (last visited 2 November 2012).
132 HPCR Commentary, above note 29, p. 94.

Literature review

In 1990, W. Hays Parks wrote: 'at this point, the standard cannot be defined in a way that is entirely satisfactory.'[133] In recent works, commentators such as Leslie Green, Judith Gardam, Ian Henderson, Dieter Fleck, Nils Melzer, and others have addressed both the definition of 'excessive' and the applicable standard – whether subjective to the mind of the commander, objective based on what a reasonable commander would do, or a combination of both.[134]

There is consensus that 'excessive' cannot be defined.[135] Because there is no conventional or customary definition, 'the decision must be made in accordance with reasonable military assessments and expectations, taking into account potential collateral damage'.[136] Excessiveness, therefore, must have an applicable standard for its determination.

A subjective standard has traditionally been the dominant viewpoint. This subjective standard asserts that a determination of excessiveness depends on that commander's good faith assessment based on the prevailing circumstances.[137] The subjective standard holds that commanders have a considerable margin of appreciation and discretion in balancing the anticipated military advantage against the expected collateral damage.[138] Accordingly, this view of the standard for determining excessiveness relies solely on that commander's available information and good faith judgement:

> [T]he rule refers to the expected rather than the actual civilian loss and the anticipated rather than the actual military advantage. In other words, the test is subjective in the sense that in judging the commander's actions one must look at the situation as he saw it and in the light of the information that was available to him.[139]

133 W. Hays Parks, 'Air war and the law of war', in *Air Force Law Review*, Vol. 32, No. 1, 1990, p. 175.

134 Bryan A. Garner (ed.), *Black's Law Dictionary*, Thompson West, St Paul, MI, 2009 ('[O]bjective standard. A legal standard that is based on conduct and perceptions external to a particular person. [S]ubjective standard. A legal standard that is peculiar to a particular person and based on the person's individual views and experiences').

135 Leslie C. Green, *The Contemporary Law of Armed Conflict*, Manchester University Press, Manchester, 2008, p. 391 ('there is no definition as to what is excessive'); D. Fleck, above note 1, pp. 178–179 ('the principle of proportionality . . . remains loosely defined and is subject to subjective assessment and balancing'); I. Henderson, above note 7, pp. 221–226 and 247; N. Melzer, above note 30, pp. 359–363; Judith Gardam, *Necessity, Proportionality and the Use of Force by States*, Cambridge University Press, Cambridge 2004, p. 98 (classifying proportionality assessment as 'imprecise').

136 L. C. Green, above note 135, p. 391.

137 N. Melzer, above note 30, p. 361; Y. Dinstein, above note 34, p. 122; J. Gardam, above note 135, pp. 105–106.

138 D. Fleck, above note 1, pp. 178–179 (The rule 'is subject to subjective assessment and balancing . . . [and] the actors enjoy a considerable margin of appreciation.'); Y. Tanaka and M. B. Young, above note 5, p. 225 ('The formulation of the proportionality rule incorporates a margin of appreciation in favor of military commanders').

139 A. P. V. Rogers, above note 32, p. 110; See also Y. Dinstein, above note 34, p. 122 ('Undeniably, the attacker must act in good faith and not simply turn a blind eye on the facts of the situation; on the contrary, he is obliged to evaluate all available information'); Y. Tanaka and M. B. Young, above note 5, p. 225.

A purely objective standard – what a 'reasonable' commander's evaluation of the anticipated military advantage, expected collateral damage, and subsequent proportionality determination would be – appears to have little support in the existing academic literature.[140] However, proponents of the subjective standard do highlight the criticism inherent in a purely subjective standard:

> The whole assessment of what is 'excessive' in the circumstances . . . is not an exact science . . . This 'subjective' evaluation of proportionality is viewed with a jaundiced eye by certain scholars, but there is no serious alternative.[141]

A subjective-objective hybrid standard provides one serious alternative. This standard asserts that while the (1) assessment of the anticipated military advantage and expected collateral damage is subjective to that commander, the (2) subsequent proportionality determination from that subjective assessment is objective:

> An assessment of the proportionality of an attack is based on the circumstances of the commander and the information available to him or her. However, the *conclusions* to be reached on whether collateral damage is *expected* and whether it is *proportional* is then based on what a reasonable person would have concluded from that information.[142]

While an objective determination from the subjective assessments is possible, the assessments nonetheless remain problematically elusive because individuals likely still: (1) value human life differently, and (2) generally value military and humanitarian interests differently.[143] Despite these problems, commanders must still make the assessments and proportionality determination with common sense and good faith, and courts may indeed hold them accountable.[144] Because an attack with excessive collateral damage engages both state and individual responsibility, there must be an objective quality to the assessment.

Judicial treatment

Recent opinions from the International Criminal Tribunal for the Former Yugoslavia (ICTY) and the Israeli Supreme Court discuss the *jus in bello* proportionality standard and the determination of 'excessiveness'.[145]

140 D. Fleck, above note 1, p. 179 ('Objective standards for the appraisal of expected collateral damage and the intended military advantage are virtually non-existent'); Y. Dinstein, above note 34, p. 122 ('There is no objective possibility of quantifying the factors of the equation, and the process necessarily contains a large subjective element').

141 Y. Dinstein, above note 34, p. 122.

142 I. Henderson, above note 7, p. 222.

143 *Ibid.*, p. 223.

144 See e.g., L. C. Green, above note 135, p. 391 ('Although the decision as to proportionality tends to be subjective, it must be made in good faith and may in fact come to be measured and held excessive in a subsequent war crimes trial').

145 Because this work focuses on the *jus in bello* proportionality rule in the conduct of hostilities, the International Court of Justice's advisory opinion, *Legality of the Threat or Use of Nuclear Weapons*, 1996 ICJ Rep. 226, will not be discussed.

The International Criminal Tribunal for the former Yugoslavia (ICTY)

In 2000 a Committee from the Office of the Prosecutor (OTP) for the ICTY investigated the North Atlantic Treaty Organization's (NATO) bombing campaign in Kosovo from March to June 1999 during Operation Allied Force.[146] Concerning allegations that NATO had 'disregarded the rule of proportionality by trying to fight a "zero casualty" war for their own side', the Prosecutor's Committee determined that NATO did not conduct an air campaign that caused 'substantial civilian casualties either directly or incidentally'.[147]

In its analysis the Committee identified, but did not solve, the following challenges to the concept of proportionality: (a) assessing the relative values between collateral damage and military advantage; (b) determining what is included or excluded in the sum totals; (c) defining the geographical and temporal limits; and (d) ascertaining whether the security of the attacking force is a factor, if any.[148] Regarding the 'excessiveness' determination, the Committee implied that it should be an objective standard based on the mind of a 'reasonable military commander'.[149]

With this framework, the Committee analysed, among other attacks, an April 1999 missile strike on the Serbian TV and Radio Station in Belgrade, which formed part of a coordinated, overall attack on the Yugoslavian command, control, and communications network.[150] NATO anticipated that the military advantage in the overall attack would be a disruption of Serbian military operations.[151] Although the analysis failed to mention NATO's 'expected' collateral damage, the actual collateral damage of this single attack consisted of between ten and seventeen civilian casualties.[152] Relative to the anticipated military advantage, the Committee determined the 'civilian casualties were unfortunately high but do not appear to be clearly disproportionate'.[153]

The Committee did not refer this attack for prosecution because it was not 'clearly disproportionate'.[154] Notably, the OTP Committee appears to have applied the Rome Statute's higher threshold of 'clearly excessive', and did not address the

146 International Criminal Tribunal for the Former Yugoslavia (ICTY), *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia*, 39 ILM 1257, November 2000, also available at: http://www.icty.org/x/file/Press/nato061300.pdf (last visited 2 November 2012).
147 *Ibid.*, paras. 2 and 54.
148 *Ibid.*, paras. 49–50.
149 *Ibid.*, para. 50 ('Although there will be room for argument in close cases, there will be many cases where reasonable military commanders will agree that injury to non-combatants or the damage to civilian objects was clearly disproportionate to the military advantage gained').
150 *Ibid.*, paras. 71–72.
151 *Ibid.*
152 *Ibid.*
153 *Ibid.*, para. 77 ('Assuming the station was a legitimate objective, the civilian casualties were unfortunately high but do not appear to be clearly disproportionate').
154 *Ibid.*

question of whether the attack was plainly excessive or disproportionate in violation of API.[155]

The ICTY's first detailed judicial inquiry into the concept of proportionality occurred in *Prosecutor* v. *Galić*. In 2003 the ICTY found Major-General Stanislav Galić guilty of war crimes and crimes against humanity, for inter alia, violating the proportionality standard during his command of the Bosnian Serb Army's twenty-three-month siege of Sarajevo, which involved a protracted sniper and shelling campaign that resulted in thousands of civilian deaths and injuries.[156] The Court adopted the OTP's objective standard for the determination of 'excessiveness':

> In determining whether an attack was proportionate it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her, could have expected excessive civilian casualties to result from the attack.[157]

For the *mens rea* element in a disproportionate attack, the Court incorporated API's standard in Article 85(3)(b) by requiring evidence that the attack was launched wilfully and in the knowledge that excessive civilian casualties would result.[158] Contrary to the OTP Committee, the Court did not hold that attacks must be 'clearly' excessive to justify prosecution, only excessive.

The Israeli Supreme Court

In 2006 the Israeli Supreme Court, sitting as the High Court of Justice, issued a judgment concerning the legality of the Israeli government's targeted killing policy that involves lethal strikes against government-labelled terrorists that incidentally killed and injured innocent civilians.[159] From 2000 to 2005 the Israeli government had killed approximately 300 'terrorists' as compared to 150 civilian deaths and hundreds of injuries.[160]

In determining that the targeted killings of Palestinian militants were legal under certain conditions, the Court held that Israel must undertake a meticulous case-by-case assessment for each attack.[161] The Court emphasized that in the

155 *Ibid.*, para. 21('The use of the word "clearly" [in the Rome Statute for Article 8(b)(iv)] ensures that criminal responsibility would be entailed only in cases where excessiveness of the incidental damage was obvious').

156 ICTY, *The Prosecutor* v. *Stanislav Galic*, Case No. IT-98-29-T, 43 ILM 794 Judgment (Trial Chamber 1), 5 December 2003, available at: http://www.icty.org/x/cases/galic/tjug/en/gal-tj031205e.pdf (last visited 2 November 2012). For a case summary, see Liza Gail, 'Introductory Note to ICTY: Prosecutor v. Galić', in *International Legal Materials*, Vol. 43, No. 4, July 2004, pp. 789–793.

157 *Ibid.*, para. 58.

158 *Ibid.*, para. 59.

159 Israel High Court of Justice, *Public Committee against Torture in Israel* v. *Israel*, HCJ 769/02, 46 ILM 375, Judgment, 11 December 2005, available at: http://elyon1.court.gov.il/Files_ENG/02/690/007/A34/02007690.A34.pdf (last visited 2 November 2012).

160 *Ibid.*

161 *Ibid.*, para. 46.

targeting assessment the proportionality standard is essentially a values-based test contingent on 'balancing between conflicting values and interests'.[162] For the determination of 'excessiveness', the Court, like the ICTY, applied an objective test based on the mind of the reasonable commander: 'the question is . . . whether the decision which the military commander made is a decision that a reasonable military commander was permitted to make'.[163]

According to the Court, some cases are easy: a missile strike on a building to take out a single combatant that kills and injures scores of civilians or bystanders would be disproportionate.[164] The hard cases are 'those which are in the space between the extreme examples'.[165] A concurring opinion also found that there may be cases where the collateral damage is 'so severe that even a military objective with very substantial benefit cannot justify it'.[166]

The International Criminal Court

The ICC's Rome Statute furthers API's criminal standard for wilful and knowing violations of the proportionality standard but, to date, this author is unaware of any successful prosecutions before the Court dealing with the principle of proportionality. Subject to other provisions of this treaty, States Party to the Rome Statute accede jurisdiction to the ICC for violations of the proportionality standard when launching an attack in the knowledge that the collateral damage would be 'clearly excessive' compared to the 'overall' military advantage anticipated.[167] This raises the threshold for the Court's prosecution beyond API's test of 'excessive' collateral damage relative to just the concrete and direct military advantage anticipated. However, the ICC's subject matter jurisdiction for attacks involving clearly excessive collateral damage is not authoritative of conventional or customary IHL.[168]

Notably, during the ICC preparatory negotiations, the US did propose a subjective-objective approach.[169] The US State Department submitted that the evaluation is 'necessarily subjective . . . based on the perspective of the accused prior to the attack', but the collateral damage must be 'manifestly excessive' (an objective standard) for criminal liability to attach.[170] The influence, if any, of this proposal, is unclear.

In conclusion, this section has traced the development of the proportionality standard and discussed its current treatment by humanitarian law experts, scholars, and jurists. The proportionality standard is critically important for the protection of civilians during armed conflict; yet the existing literature fails to

162 *Ibid.*, para. 45.
163 *Ibid.*, para. 57.
164 *Ibid.*, para. 46.
165 *Ibid.*
166 *Ibid.*, Concurring Opinion, para. 5 (Rivlin, J.).
167 Rome Statute, above note 94, Art. 8(2)(b)(iv) (emphasis added).
168 Rome Statute, above note 94, Art. 10; ICRC Study, above note 9, p. 577.
169 Proposal Submitted by the USA to the Preparatory Committee on the Establishment of an International Criminal Court, UN Doc. A/AC.249/1998/DP.11, 2 April 1999.
170 *Ibid.*, p. 13.

provide clarity or an adequate framework for determining what would be excessive in a given attack. Nonetheless, for planners, legal advisers, and commanders, '[d]espite the difficulty of that balancing, there's no choice but to perform it'.[171]

The courts and HPCR suggest an objective 'reasonable commander' standard, whereas the ICRC Commentary of API appears to propose a subjective standard, and several scholars propose a subjective standard relative to the mind of that commander. The final section reconciles the viewpoints on the standard for determining what is excessive and presents the subjective-objective test as the preferred model. A targeting checklist for deliberate (or planned) lethal targeting missions is then provided for the *jus in bello*.[172]

While the legal analysis remains the same for international and non-international armed conflicts, additional attention is devoted to counter-insurgencies as a type of non-international armed conflict. Even though a comprehensive analysis of comparative state practice is beyond the scope of this article, evaluation of US state practice presents a useful example of a state that has been actively engaged in targeting. For more than a decade, the US has conducted counter-insurgencies operations in Afghanistan, and recently concluded such operations in Iraq. Consideration of modern US state practice, therefore, may assist in framing the argument that all states (and belligerents other than armed forces of a state) would benefit from refining their institutional mechanisms and methodology for targeting and proportionality assessments.

Operational framework: a proposed methodology for determining what is excessive

> Wherever an army is stationed, briars and thorns spring up . . . A skilful commander strikes a decisive blow, and stops . . . but will be on his guard against being vain or boastful or arrogant in consequence of it. He strikes it as a matter of necessity; he strikes it, but not from a wish for mastery.
>
> Tao Te Ching[173]

Military lawyers advising planners and commanders on lethal targeting decisions must be experts in IHL and the specific provisions governing attacks and the protection of the civilian population for international and non-international armed conflicts. For COIN operations as a type of non-international armed conflict, legal advisers should also understand COIN theory and doctrine. The US has engaged in significant COIN operations for the past decade and, therefore, its doctrine has been refined by practice. Most importantly for present purposes, COIN doctrine provides

171 Public Committee, above note 159, para. 46.

172 For a discussion of the *jus ad bellum* and targeting, see N. Melzer, above note 30, pp. 51–54, or J. Gardam, above note 135, Chaps. 5 and 6.

173 Lao Tzu, *The Tao Te Ching*, verse 30, available at: http://ebooks.adelaide.edu.au/l/lao/tzu/l2988t/ (last visited 2 November 2012).

specific targeting guidance with a stated aim of protecting the civilian population. Its emphasis on minimizing civilian harm provides a useful application of operational theory heeding the tenets of core international humanitarian law principles.

Lethal targeting in counterinsurgencies: US doctrine examined

COIN is an extremely complex type of warfare where the fundamental purpose is to win the trust and confidence of the population; therefore, '[t]he protection, welfare, and support of the people are vital to success'.[174] To achieve these desired effects, a synchronized targeting staff cell (which includes a legal adviser) is one tool that a commander uses to develop and prioritize lethal and non-lethal target sets:

> Effective targeting identifies the targeting options, both lethal and non-lethal, to achieve effects that support the commander's objectives. Lethal targets are best addressed with operations to capture or kill; non-lethal targets are best engaged with [civil-military operations, information operations], negotiation, political programs, economic programs, social programs and other non-combat methods.[175]

For instance, an example of a proposed lethal target could be a member of the enemy state's armed forces. An example of a non-lethal target could be supporting a job-growth programme for disenfranchised youth or developing a disarmament, demobilization, and reintegration programme for insurgents who have laid down their arms. Specific to lethal targeting, COIN theory provides that a state's own combatants must not only minimize harm to the civilian population, but should '[a]ssume additional risk to minimize potential harm'.[176]

The Army's COIN manual characterizes the proportionality test in conventional operations as 'usually calculated in simple utilitarian terms: civilian lives and property lost versus enemy destroyed and military advantage gained'.[177] For COIN operations, the assessed military advantage should not be how many insurgents are killed or captured, but which insurgents.[178] Consequently, in the COIN context, the proportionality balance for attacks against an individual insurgent should be: 'the number of civilian lives lost and property destroyed . . . measured against how much harm the targeted insurgent could do if allowed to escape'.[179] Because the military advantage may be lessened for a relatively inconsequential insurgent, 'then proportionality requires combatants to forego severe action, or seek non-combative means of engagement'.[180]

174 COIN Manual, above note 83, para. 159.
175 *Ibid.*, paras. 5 and 100–103.
176 *Ibid.*, para. 7–30.
177 *Ibid.*, para. 7–32.
178 *Ibid.*
179 *Ibid.*
180 *Ibid.*

Where lethal force is used, COIN commanders should evaluate not only the desired effects of the action, but also possible undesired secondary and tertiary outcomes:

> For example, bombs delivered by fixed-wing close air support may effectively destroy the source of small arms fire from a building in an urban area; however, direct-fire weapons may be more appropriate due to the risk of collateral damage to nearby buildings and non-combatants.[181]

Consequently, COIN operations should avoid 'the use of area munitions to minimize the potential harm inflicted on non-combatants located nearby'.[182]

Nevertheless, the COIN manual specifies that precision air attacks are a valuable asset, but commanders must weigh the benefits of each air strike against the potential risks.[183] Beyond causing non-combatant casualties as an undesired effect, the secondary effects could consist of (a) alienating the populace against the pro-government forces, (b) providing a major propaganda victory for insurgents, and (c) generating 'media coverage that works to the insurgents' benefit'.[184] Finally, a tertiary effect could ultimately be a strengthened insurgency: '[Lethal f]ires that cause unnecessary harm or death to non-combatants may create more resistance and increase the insurgency's appeal – especially if the populace perceives a lack of discrimination in their use'.[185]

For these reasons, COIN theory requires commanders to evaluate the ethical, moral, and practical implications of the use of force and the proportionality standard in action.[186] Concerning the efficacy of air strikes, commanders 'should consider the use of air strikes carefully during COIN operations, neither disregarding them outright nor employing them excessively'.[187]

COIN theory, in sum, is fundamentally a macro-prospective on how practitioners should think about targeting and proportionality assessments; it is a balance of military interests versus humanitarian interests where the scale should always tip in favour of humanity.

What is 'excessive'?

As the commentaries, scholars, and jurists convey, 'excessive' cannot be defined or quantified, but may be qualitatively assessed based on an applicable standard – whether subjective to the mind of the commander, objective based on a reasonable commander approach, or a hybrid of the two. This author believes that Henderson's hybrid approach, the subjective-objective model, functionally reconciles the discord

181 *Ibid.*, para. 7–36.
182 *Ibid.*
183 *Ibid.*, p. E-1.
184 *Ibid.*
185 *Ibid.*, para. 7–37.
186 *Ibid.*
187 *Ibid.*, p. E-2.

among the ICRC, HPCR experts, commentators, and courts, and provides a legally sufficient framework for both international and non-international armed conflicts.

Henderson's subjective-objective model deconstructs the proportionality test into two parts: (1) a subjective assessment by the commander of the anticipated military advantage (AMA) and the expected collateral damage (ECD) and (2) an objective determination based on the balancing of these interests from the perspective of a 'reasonable military commander'.[188] In other words, planners and commanders must evaluate in good faith the anticipated military advantage and expected collateral damage in light of the circumstances prevailing at the time. Based on this subjective assessment, the resulting balancing must be objectively reasonable in ensuring that the civilian deaths, injury, or property destruction are not excessive.

Aside from the importance of having a standard to apply in furthering the protection of the civilian population, belligerents should be on notice as to when criminal liability attaches. In this respect it is worth noting that the IHL rule differs slightly from its international criminal law counterpart in the Rome Statute.[189] For state responsibility under IHL, the attack need only be disproportionate, and an individual may be prosecuted for a grave beach where the attack is launched with the knowledge that such disproportionate effects would result.[190] The ICC criminal standard, on the other hand, requires the effects to be 'clearly' disproportionate (relative to the overall anticipated military advantage) before an individual may be prosecuted for a disproportionate attack.[191]

Determining 'excessiveness': a proposed institutional model

This author believes that Henderson's model may be extended further. Using the preferred, hybrid subjective-objective standard, common reference points could assist legal advisers in classifying both the anticipated military advantage and the expected collateral damage to determine what is excessive for a grave breach in international humanitarian law or 'clearly excessive' per the ICC.

For part one of the subjective-objective approach – the good faith subjective assessment of both the anticipated military advantage and the expected collateral damage – both variables could be scaled or given ranges to determine whether the respective values are marginal, moderate, or substantial. Once the anticipated military advantage and the expected collateral damage have subjective values, then these values may be objectively weighed.

For instance, consider a scenario where there are thirty-five, fortified enemy soldiers with four light-armoured vehicles, and one tank blocking a critical bridge crossing in a major city where enemy forces control 35 per cent of the city. There is three-story apartment building next to the bridge and enemy emplacement.

188 I. Henderson, above note 7, p. 223.
189 Amichai Cohen and Yuval Shany, 'A development of modest proportions – the application of the principle of proportionality in the targeted killings case', in the *Journal of International Criminal Justice*, Vol. 5, No. 2, May 2007, p. 319.
190 API, above note 3, Art. 85.
191 Rome Statute, above note 94, Art. 8(b)(iv).

Based on human geography trends for the area and other intelligence (for example, geospatial imagery, etc.) there is a good faith basis to believe that the apartment building contains at least nine apartment units, and that anywhere from thirty-six to seventy-two civilians may be inside at any given time of the day.

Neutralizing these enemy soldiers and their armoured assets allows for freedom of movement for allied forces and will set the conditions for allied forces to take clear the area of enemy forces, hold the territory, and build on the gains. It is expected that a lethal strike on this emplacement by air poses the smallest risk of incidental harm to the civilian population, and that based on the weaponeering assessment and likely structural integrity of the building, the blast radius could damage 15 per cent of the building and potentially kill or seriously wound any residents on the blast side of the building – anywhere from four to nine civilians.

What decision should the commander make? What is the legal advice? Clearly, targeting and proportionality assessments must be made on a case-by-case basis, in good faith, and in light of the circumstances prevailing at the time. What is generally lacking from state practice, however, is a method for this life and death decision. The following table proposes a method.

The assumption underlying this table is that a commander will apply good faith and common sense when attributing values in the assessment.[192] Nonetheless, providing some semblance of order and objectivity in a proportionality assessment would provide useful clarity on this difficult question. On these assumptions, where there is an imbalance in the values (assessed in good faith and with common sense), such as a moderate anticipated military advantage versus a substantial expected collateral damage, the attack would be objectively 'excessive' under IHL and the attacking force must refrain from the attack. If the attack is nonetheless carried out wilfully in the knowledge that it is disproportionate, the state and responsible individual(s) will have committed a grave breach of API.

Where a significant imbalance between the values exists, such as a marginal anticipated advantage and a substantial expected collateral damage, the attack would be 'clearly excessive'; if carried out, the state and responsible individual(s) would certainly have committed a grave breach, and the individuals ordering the attack may be criminally liable.

A legally complex issue arises where both the anticipated military advantage and expected collateral damage would be substantial. Recall again that with respect to determining what is 'excessive' the ICRC Commentary asserts that API 'does not provide any justification for attacks which cause extensive civilian losses and damages', irrespective of a comparative anticipated military advantage, because '[i]ncidental losses and damages should never be extensive'.[193] A concurring justice

192 While the anticipated military advantage in an attack will always vary in light of prevailing circumstances at the time based on tactical, operational, and strategic objectives, national militaries may find it useful to establish objective guidelines concerning what amount of civilian death, injury, or destruction would generally be marginal, moderate, and substantial (e.g., 0–1 anticipated civilian casualties is marginal, 2–4 is moderate, and 5+ is substantial).

193 ICRC Commentary, above note 14, p. 626, para. 1980.

from the Israeli High Court of Justice also holds this view, that there may be cases where the collateral damage is 'so severe that even a military objective with very substantial benefit cannot justify it'.[194] However, the HPCR experts disagree with these assertions that 'extensive' collateral damage is prohibited in all circumstances: 'extensive collateral damage may be legally justified by the military value of the target struck, because of the high military advantage anticipated by the attack'.[195]

To the extent there exists debate, the answer should err on the side of maximizing the protections of the civilian population – in accordance with the principles of humanity and dictates of public conscience. These rules exist to strike a balance between the military exigencies of war and the requirements of humanity. War should never trump our humanity. In other words, 'if it comes to a choice between being a good soldier and a good human being – try to be a good human being'.[196]

Turning now to the analysis for COIN warfare, where the values between the anticipated military advantage and the expected collateral damage remain the same and thus proportionate, US state practice would oblige commanders to refrain from launching the attack. For operational reasons, doctrine would permit commanders in COIN environments to consider lethal attacks where the anticipated military advantage is substantial and the expected collateral damage is either marginal or moderate, and where the anticipated military advantage is moderate and the expected collateral damage is marginal.

There is no easy answer to the question posed at the outset of this section, but – '[d]espite the difficulty of that balancing, there's no choice but to perform it'.[197] As a matter of state practice, institutional mechanisms, such as clarifying the definition for what constitutes excessive collateral damage and adopting a framework to assist in resolving real-life situations like the hypothetical ones advanced above, would assist those involved in these difficult life and death decisions on a case-by-case basis and overall in lessening the conceptual confusion.

Determining 'excessiveness' is only one of the crucial steps in a targeting process that starts with applying international humanitarian law (as opposed to starting off and relying nearly exclusively on rules of engagement). The following section provides a consolidated checklist to apply to assist legal advisers and other practitioners.

Targeting legal analysis: seven steps

Military practitioners cannot rely solely on any applicable rules of engagement or collateral damage methodology when legally reviewing a planned lethal attack. When conducting a legal review for staff officers and commanders, legal advisers

194 Public Committee, above note 158; Concurring Opinion, para. 5. (Rivlin, J.).
195 HPCR Commentary, above note 29, p. 92.
196 Anton Myrer, *Once an Eagle*, HarperCollins, New York, 1968, p. 1288.
197 Public Committee, above note 159, para. 46.

must apply the international legal rules that govern attacks. The following steps may guide such an analysis.[198]

Step 1: valid military objective[199]

Ensure the target is a valid military objective that is not otherwise protected from attack under IHL.[200] Though there are nuances in status determinations for belligerents engaged in either international armed conflict and non-international armed conflict, this generally includes a determination as to whether an individual is subject to attack, such as a soldier who is part of the armed forces of an enemy, or a civilian who has lost immunity from attack by taking direct part in the hostilities.[201]

Determination of a military object involves a two-part test: (a) does the object, based on its nature, location, purpose, or use, make an effective contribution to the enemy's military action (objective analysis); and (b) does its neutralization present a definite military advantage based on the current circumstances (subjective analysis)?[202]

Step 2: distinction/intelligence gathering[203]

Assess the intelligence on the target, its location, and surroundings (that is, civilians and civilian objects), ensure the intelligence is continually updated and review any updated intelligence prior to any attack.

Step 3: non-lethal alternative[204]

For this 'lesser of two evils' rule, determine whether there is a non-lethal alternative (that is, other courses of action) to the lethal attack that will achieve the same concrete and direct anticipated military advantage. Consistent with recent US state practice, ask: 'can action be taken without endangering civilians . . . [and] are other options available?'[205]

198 These steps are extracted from API Art. 48–57; see also, I. Henderson, above note 7, pp. 237–238; N. Melzer, above note 30, pp. 419, 427.

199 API, above note 3, Arts 48, 50, 51, 52, and 57(2)(a)(i).

200 API, above note 3, Art. 52(2) ('In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offers a definite military advantage').

201 For a concise discussion on the rules governing the targeting of civilians who may be part of an irregular armed group, see HPCR Commentary, above note 29, pp. 117–124. See also, ICRC, *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law* (2008), above note 25.

202 HPCR Commentary, above note 29, p. 49 (Definite 'exclude[s] advantage which is merely potential, speculative, or indeterminate').

203 API, above note 3, Arts 48, 51(2), 52, and 57(2)(a)(i).

204 API, above note 3, Arts 57(1) and 57(a)(2)(ii).

205 Civilian Casualty Mitigation, above note 90, para. 2–54 (Rules of Engagement Considerations) this third step is arguably *lex feranda*); see Michael N. Schmitt, 'Book review: targeted killing in international law', in

Step 4: feasible precautions[206]

Undertake all feasible precautions to minimize the expected collateral damage. This includes warning the civilian population of an attack to facilitate evacuation and considering the choice of weapons and method of attack. If the element of surprise is required for the attack, then the attacking force should put the civilian population on notice as to what types of facilities or conduct would potentially subject them to direct attack. Other variables that bear on this step include:

> Their location (possibly within or in the vicinity of a military objective), the terrain (landslides, floods etc.), accuracy of the weapons used (greater or lesser dispersion, depending on the trajectory, the range, the ammunition used etc.), weather conditions (visibility, wind etc.), the specific nature of the military objectives concerned (ammunition depots, fuel reservoirs, main roads of military importance at or in the vicinity of inhabited areas etc.), technical skill of the combatants (random dropping of bombs when unable to hit the intended target).[207]

Step 5: proportionality test[208]

Perform the proportionality test by determining whether the expected collateral damage would be excessive or disproportionate to the anticipated military advantage. This is a two-part test using the subjective-objective approach.

For part one, the subjective assessment, in good faith and in light of the available information at the time, place a subjective value (for example, marginal, moderate, or substantial) on both the anticipated military advantage and the expected collateral damage. For the temporal element, consider from both the short- and long-term perspective, taking into account secondary and tertiary effects. Foreseen indirect effects on the civilian population should be factored into the analysis.[209]

For part two, the objective determination, refer to the Table 1 hereafter and compare these values to determine whether the result would be proportionate or excessive from the perspective of a 'reasonable military commander'. As an institutional mechanism, belligerents should attempt to define or otherwise provide

American Journal of International Law, Vol. 103, No. 4, October 2009, pp. 817–818. However, the non-international conflict of counterinsurgency warfare requires this consideration as a matter of US state practice. HPCR Commentary, above note 29, pp. 44 and 91. (For definitions, concrete and direct 'refers to military advantage that is clearly identifiable and, in many cases, quantifiable . . . it cannot be based merely on hope or speculation', and military advantage 'means those benefits of a military nature that result from an attack . . . relat[ing] to the attack considered as whole and not merely to isolated or particular parts of the attack'.)

206 API, above note 3, Art. 57.

207 ICRC Commentary, above note 14, p. 684, para. 2212. HPCR Commentary, above note 29, p. 38 (Feasible 'means that which is practicable or practically possible, taking into account all circumstances prevailing at the time, including humanitarian and military considerations').

208 API, above note 3, Arts 51(5)(b) and 57(2)(a)(iii).

209 HPCR Commentary, above note 29, p. 91.

Table 1. *A model for qualifying the anticipated military advantage and the expected collateral damage under international humanitarian law*

		EXPECTED COLLATERAL DAMAGE		
		MARGINAL	MODERATE	SUBSTANTIAL
MILITARY ADVANTAGE	MARGINAL	Proportionate ***[Refrain in COIN]***	Excessive (Per IHL)	Clearly Excessive (Per IHL & ICC)
	MODERATE	Proportionate	Proportionate ***[Refrain in COIN]***	Excessive (Per IHL)
	SUBSTANTIAL	Clearly Proportionate	Proportionate	**Proportionate?** ***[Refrain in COIN]***

useful reference points for attempting to define these values (such as marginal, moderate, or substantial). Absent an institutional model, this approach may be used on a case-by-case basis, but it is recommended that 'commanders at higher levels may want to reserve for themselves the approval authority for operations that have an excessively high risk of civilian casualties'.[210] To put the consequences into perspective, it may be useful to encourage decision-makers to imagine that those civilians subject to potential harm are those from their very own hometown, or their high school, or even their own family and friends.

Step 6: cancellation or suspension[211]

Ensure the tactical operators know to cancel or suspend the attack if the target is no longer a valid military objective (for example, *hors de combat*), if the target cannot be positively identified, or if other circumstances would make the attack

210 Civilian Casualty Mitigation, above note 90, para. 2–33.
211 API, above note 3, Art. 57(2)(b).

disproportionate (for example, earlier assessment of collateral damage changes with increased civilian presence).

Step 7: diligent execution[212]

Ensure the tactical operators, such as air pilots, artillerymen or drone pilots, diligently execute the attack by taking appropriate care to hit the desired aim point with the least amount of collateral damage.

Conclusion

> If a man is slain unjustly, his heir shall be entitled to satisfaction. But let him not carry his vengeance to excess, for his victim is sure to be assisted and avenged.
>
> The Qur'an[213]

To answer the question posed at the outset: there is no overarching definition of 'excessive' because the variables in the proportionality standard are relative to each other. Commanders must consider each attack on a case-by-case basis, and for this reason, there can be no bright-line rule.

However, a standard for determining what is excessive may be defined. As this analysis reveals, the proposed standard would find any outcome excessive that is objectively 'unreasonable' based on a commander's subjective assessment of the anticipated military advantage and the expected collateral damage. Commanders, military planners, and legal advisers would benefit from employing this subjective-objective hybrid model in deciding whether an attack is proportionate. Because objectivity varies, institutions should consider applying a common lexicon in weighting the subjective values of the anticipated military advantage and the expected collateral damage along a scale, such as marginal, moderate, or substantial.

While the proportionality standard provides constructive ambiguity, the scale should always be tilted in favour of furthering the protection of the civilian population. To accomplish this, military practitioners who provide legal advice on lethal targeting decisions must develop a keen understanding of IHL. Knowing the four basic principles of IHL is necessary, but far from sufficient. Deliberate targeting with lethal force not only requires the application of any relevant rules of engagement and collateral damage methodology, but also adherence to the specific IHL rules that govern attacks and the protection of the civilian population. Beyond complying with these legal and policy obligations, military lawyers advising in COIN operations must understand COIN theory. Excessive collateral damage not only increases human suffering, but it undermines strategic military aims.

Clearly, the most difficult question in any targeting analysis occurs when some unfortunate, incidental civilian death, injury, or property damage is

212 API, above note 3, Arts 48 and 51(4)(a).
213 The Holy Qu'ran, verse 17:31.

anticipated in an attack on a valid military objective. As Abraham asked the Lord, what amount of death and destruction is excessive? Because this is fundamentally an abhorrent question, it defies an easy answer – but this answer, regrettably, must be reached.

A standard for determining what is excessive collateral damage has evolved since its initial formulation in the Lieber Code, and it will continue to evolve. With the rise of international criminal law, it can no longer be argued that the proportionality analysis is purely subjective in the mind of the commander. Because the fog of war will always remain an inextricable aspect of armed conflict, commanders in the heat of battle will place different values on military objectives based on the information available to them at the time. For this reason the proportionality analysis cannot be wholly objective. The standard, therefore, is a hybrid subjective-objective test.

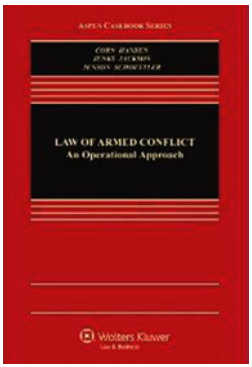
To assist in the analysis, it is possible to assign basic values – such as marginal, moderate, and substantial – to both variables throughout the analysis. Although described above in antiseptic, legal language, what is at stake is nothing less than the horrendous suffering of ordinary innocent people. Modern warfare – whether international or non-international armed conflict – has the potential to magnify this suffering because belligerents often operate from within population centres. The use of the hollow term 'collateral damage' for civilian deaths fails to incorporate the key concept that it justifies killing the very people who should be protected. This deficiency is not lost on military strategists, such as COIN strategists, or on the civilian population – 'collateral damage', quite simply, has the capacity to fuel further violence.

To this end, this article has attempted to assist fellow counsellors at law and in arms in applying greater fidelity to the overall targeting analysis while paying critical attention to the difficult proportionality standard. As the first-line defenders of human rights in combat environments, commanders want your counsel. Stand up and be heard.

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

BOOKS AND ARTICLES



The law of armed conflict: an operational approach

Geoffrey S. Corn, Victor Hansen, Richard Jackson, Christopher Jenks, Eric Talbot Jensen, James A. Schoettler*

Book review by Jamie A. Williamson, Legal Adviser, Advisory Services on International Humanitarian Law, ICRC

Any author who decides to embark on writing a textbook will be confronted by many considerations in terms of materials as well as demands from students and academics. The materials presented must be coherent, relevant and sound. Professors will scrutinise these as they look for 'the' book that will help them successfully teach and structure a course. A textbook must obviously also be of interest to students, digestible and ideally stimulating, even if the subject matter cannot always be so. Indeed, a bored student is one of the least wanted audiences for professors. Beyond the lecture halls and seminar rooms, textbooks can also serve as useful references for other academics and practitioners in the field. Their needs will be more pointed, and, even if they are not seen as the prime audience for the book, their endorsement can do no harm.

The recently published textbook, entitled '*The Law of Armed Conflict: An Operational Approach*', succeeds in meeting most, if not all, of these goals. It is a timely addition to the teaching of the law of armed conflict (LOAC), also known as international humanitarian law (IHL).[1] Written from an 'operational' perspective and very much influenced by United States practice and policy, it provides important insight into the thinking of military lawyers in applying the laws of war.

* An Aspen Casebook Series, Published by Wolters Kluwer, Law & Business, 2012. The views expressed here are those of the book reviewer alone and not of the International Committee of the Red Cross.

doi:10.1017/S1816383112000781

The textbook is well written, substantive and thought-provoking; and takes a practical approach by submersing students in the world of operational lawyers.

Until the mid-1990's, the laws of war were given relatively scant attention by universities and law schools, in particular in the United States. Those most familiar with the laws of war, compared to today, were few, and traditionally limited to members either of the armed forces or of international humanitarian organisations such as the International Committee of the Red Cross (ICRC) and Non Governmental Organizations (NGOs). Experts from these groups could speak eloquently and at length on such fundamental principles as distinction, proportionality and precaution, balancing military necessity with humanitarian considerations and debating such concepts as unnecessary suffering.

However, with the experiences in Somalia, Rwanda, Darfur and the former Yugoslavia, recurring hostilities in Gaza and Israel, the advent of international criminal tribunals, 9/11, the subsequent conflicts in Afghanistan and Iraq, and detention in Guantanamo, all amplified by 24/7 media coverage, this body of law has become of interest to a growing number of policy makers, judges, lawyers, students and academics. Indeed, debates about the applicability of Common Article 3 to detainees made front-page news, the Geneva Conventions appeared in *Vanity Fair* Magazine[2], drones stretched the battlefield for everyone to see, and cyber warfare left the confines of Silicon Valley to become actuality. These days, everyone can have an opinion on the laws of war, their relevance and meaning in modern-day armed conflicts. In many ways, as a consequence of the shifting of the debate from the battlefield to the mainstream, the laws of war have now become a subject of particular interest in Universities and many Law Schools.

Thus, the first challenge with any new textbook on the laws of war is to bring to the fore all of these issues whilst not omitting the fundamentals. This book does not fail in this regard. It is divided into 14 main chapters covering everything from the legal bases for use of force (chapter 1) and the history and sources of the law of armed conflicts (chapter 2), the triggering of the law of armed conflict (chapter 3) before delving into the core of the subject and discussing all of the core concepts of the laws of war. There is also a fine Chapter on Naval Warfare and the Law of Neutrality (chapter 12), subjects which are often neglected in most mainstream academic treatise.

Building on solid foundations, the authors have also given themselves the room to consider those areas of the law that are being tested by modern armed conflicts. Many questions, as the authors demonstrate, remain contentious and in many ways unresolved. Whilst not every reader will necessarily agree with some of the viewpoints expressed by the authors, by tackling these more litigious issues and presenting the various sides of the debates in a balanced manner, the textbook is suitably enriched.

1 For the purposes of this review, the term laws of war will be used to cover the Law of Armed Conflict 'LOAC' (a label generally preferred by military lawyers) and International Humanitarian Law (a label generally preferred by civilian humanitarian lawyers).

2 See for instance Philippe Sands, 'The Green Light', in *Vanity Fair*, available at http://www.vanityfair.com/politics/features/2008/05/guantanamo200805.

Chapters 3–6, and 10, are noteworthy in this regard. In Chapter 3, which considers the triggering of LOAC, traditionally seen as the existence of either an international or a non-international armed conflict, the authors also allow for a discussion of the concept of 'transnational armed conflicts against non-state actors', underscoring both the legal as well as operational complexities of the issues at stake. A forceful argument is made in this section of this book in favour of this concept, even though it has not been fully endorsed elsewhere.[3]

Chapter 5 considers *inter alia* the concept of direct participation in hostilities, which, as we know, still gives rise to some unsettled issues, despite the efforts of the ICRC and many of the best intellects, practitioners as well as academics in this field. Some of the responses to the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, which were published notably in the *New York Journal of International Law and Politics* bring to light the areas of divergence.[4] The authors of the book could have rekindled many of the emotive disagreements, yet to their credit, they have tackled the issues dispassionately. Similarly, in Chapter 6, room is made for discussion on the concept of 'unprivileged belligerent', a category of individuals which the authors recognise is 'controversial and currently rejected by a majority of states'. And Chapter 10 highlights the controversies surrounding the legal basis for detention of individuals arrested in the framework of the so called 'global war on terror'.

The inclusion and discussion of these somewhat more sensitive concepts, even if there is no universal consensus on their meaning, enriches the book. There is a sufficient breadth of references in the book so as to allow the students to read the diverse views on such issues, and to form their own opinion.

3 See for instance ICRC, 'International Humanitarian Law and the challenges of contemporary armed conflicts', Report prepared by the ICRC, 31st International Conference of the Red Cross and Red Crescent, December 2011, available at: http://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf (all last visited October 2011).

4 The ICRC Guidance is available at: http://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf. See also in *New York University Journal of International Law & Politics*, Vol. 42, No. 3, Spring 2010: Ryan goodman & Derek Jinks, 'The ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law: An Introduction to the Forum', pp. 637–640, available at: http://www.law.nyu.edu/ecm_dlv4/groups/public/@nyu_law_website__journals__journal_of_international_law_and_politics/documents/documents/ecm_pro_065929.pdf; Kenneth Watkin, 'Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance', pp. 641–695, available at: http://www.law.nyu.edu/ecm_dlv4/groups/public/@nyu_law_website__journals__journal_of_international_law_and_politics/documents/documents/ecm_pro_065932.pdf; Michael N. Schmitt, 'Deconstructing Direct Participation in Hostilities: The Constitutive Elements', pp. 697–739, available at: http://www.law.nyu.edu/ecm_dlv4/groups/public/@nyu_law_website__journals__journal_of_international_law_and_politics/documents/documents/ecm_pro_065931.pdf; Bill Boothby, '"And for Such Time As": The Time Dimension to Direct Participation in Hostilities', pp. 741–768, available at: http://www.law.nyu.edu/ecm_dlv4/groups/public/@nyu_law_website__journals__journal_of_international_law_and_politics/documents/documents/ecm_pro_065933.pdf; W. Hays Parks, 'Part IX of the ICRC "Direct Participation in Hostilities" Study: No Mandate, No Expertise, and Legally Incorrect', pp. 769–830, available at: http://www.law.nyu.edu/ecm_dlv4/groups/public/@nyu_law_website__journals__journal_of_international_law_and_politics/documents/documents/ecm_pro_065930.pdf; Nils Melzer, 'Keeping the Balance between Military Necessity and Humanity: A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities', pp. 831–916, available at: http://www.law.nyu.edu/ecm_dlv4/groups/public/@nyu_law_website__journals__journal_of_international_law_and_politics/documents/documents/ecm_pro_065934.pdf.

The second challenge for any book is to make it intellectually accessible to students and practical for professors. As a teaching tool, the authors have opted for a more 'hands-on', rather than a purely theoretical, approach. Throughout the chapters, the book develops on an 'overarching hypothetical scenario . . . loosely based on the 1989 U.S. Military Operations in Panama', code named Operations Just Cause and Promote Liberty. Students are expected to take on the role of a junior JAG officer participating in the various operations, advising their commander and staff on legal issues in the 'planning and execution of a wide array of combat and post-combat operation.' As the scenario evolves, it builds on the knowledge that the students acquire chapter by chapter. From having to advise on different military operations, the legal obligations of U.S. forces, and on collateral damage assessments, to receiving briefings at the Pentagon, and deciding when to terminate hostilities, there is little respite for the students as they work through the materials. Questions abound, testing the reader's understanding of the law and operational challenges, in a very dynamic fashion.

From the opening volley of questions, where the President asks, 'all right, we have been watching this situation pretty close for a while. I want to know what everyone thinks', after having been briefed on assaults against U.S. servicemen by members of the Panamanian Defence Force, the student is drawn into a page turning law of war thriller, where s/he can play a lead role. As a teaching tool therefore, this book is not only intellectually stimulating but also pushes the students to think practically about the law, which, in many ways, is an essential exercise in the honing of work skills.

Lastly, if a book is to stand out from others on the same subject, it needs to bring something different to the table. Here, it is the fact that the authors have proffered an 'operational approach' to their material. As they explain, 'it is the ability to apply the law to the problems presented during military operations that defines success, and an appreciation of the complexity of this intersection of law and operations will contribute to positive development in the law.'

With over 120 years combined U.S. military experience, the authors have a privileged vantage point, of having first-hand experience in the application by the U.S. of the laws of war during armed conflicts. The injection of their insights and fruits of their operational experience into the materials makes the book unique. To be sure, some readers may feel that the book comes across as overly U.S.-centric. However, this is actually one of the strong elements of this book, in that it provides invaluable insight into U.S. thinking and operational law, which have influenced the U.S. military and policy makers over the past few years. The authors have not sought to argue that the U.S. position should always be the standard-bearer. Instead, they have succeeded in finding the right balance between theory and the practice, and to bring to light the operational realities of the laws of war, with a focus on U.S. policy and military doctrine.

In conclusion, this book is an important addition to today's teaching on the laws of war. The authors have taken the time and space to review objectively the development and status of the laws of war, whilst also managing effectively to bring to the fore the many challenges and dilemmas faced by operational military lawyers.

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

BOOKS AND ARTICLES

New publications in humanitarian action and the law

This selection is based on the new acquisitions of the ICRC Library and Public Archives

Arms – books

Cimbala, Stephen J. *Nuclear weapons in the information age*. London and New York: Continuum, 2012, 238 pp.
Cooper, Neil, and Mutimer, David (eds). *Reconceptualising arms control: controlling the means of violence*. London and New York: Routledge, 2012, 268 pp.
Millett, Piers (ed.), *Improving implementation of the Biological Weapons Convention: the 2007–2010 intersessional process*. New York and Geneva: UNIDIR, 2011, 299 pp.
Moreau, Virginie. *Le traité sur le commerce des armes: les enjeux pour 2012*. Bruxelles: GRIP, 2011, 35 pp.

Arms – articles

Brunstetter, Daniel and Braun, Megan. 'The implications of drones on the just war tradition', *Ethics and International Affairs*, Vol. 25, No. 3, 2011, pp. 337–358.
Hashey, Philip. 'White phosphorous munitions: international controversy in modern military conflict', *New England Journal of International and Comparative Law*, Vol. 17, 2011, pp. 291–315.
Nicoulaz, Myriam. 'Les armes à sous-munition: le conflit israélo-libanais de l'été 2006 et la genèse d'un traité', *Schweizerische Zeitschrift für internationales und europäisches Recht = Revue suisse de droit international et de droit européen = Rivista svizzera di diritto internazionale e europeo = Swiss Review of International and European Law*, 21e année, No. 4, 2011, pp. 647–667.
Wuschka, Sebastian. 'The use of combat drones in current conflicts: a legal issue or a political problem ?', *Goettingen Journal of International Law*, Vol. 3, No. 3, 2011, pp. 891–905.

doi:10.1017/S1816383112000501

Children – books

de Ruiter D. (ed.). *The rights of children in international criminal law: children as actor and victim of crime*, [s.l.]: International Courts Association, 2011, 332 pp.
Drumbl, Mark A. *Reimagining child soldiers in international law and policy*. Oxford: Oxford University Press, 2012, 239 pp.
Grover, Sonja C. *Child soldier victims of genocidal forcible transfer: exonerating child soldiers charged with grave conflict-related international crimes*. Heidelberg: Springer, 2012, 302 pp.
Roman, Victor. *Should child soldiers be punished for war crimes? Inspired by the case of Omar Khadr*. Saarbrücken: Lap Lambert Academic, 2011, 69 pp.
UNICEF. *Estado mundial de la infancia 2012: niñas y niños en un mundo urbano*. New York: UNICEF, 2012, 142 pp.
UNICEF. *La situation des enfants dans le monde 2012: les enfants dans un monde urbain*. New York: UNICEF, 2012, 142 pp.
UNICEF. *The state of the world's children 2012: children in an urban world*. New York: UNICEF, 2012, 142 pp.

Children – articles

Johnson, Kirsten *et al.* 'From youth affected by war to advocates of peace, round table discussions with former child combatants from Sudan, Sierra Leone and Cambodia', *Journal of International Peacekeeping*, Vol. 16, Nos. 1–2, 2012, pp. 152–174.
'Protecting children in armed conflict: a conversation with Radhika Coomaraswamy', *Fletcher Forum of World Affairs*, Vol. 36, No. 1, Winter 2012, pp. 5–8.

Civilians – books

Doss, Alan. *Great expectations: UN peacekeeping, civilian protection, and the use of force*. Geneva: Geneva Centre for Security Policy, December 2011, 43 pp.

Civilians – articles

Christian, Mervyn *et al.* 'Sexual and gender based violence against men in the Democratic Republic of Congo: effects on survivors, their families and the community', *Medicine, Cconflict and Survival*, Vol. 27, No. 4, October–December 2011, pp. 227–246.
de Waal, Alex, Meierhenrich, Jens, and Conley-Zilkic, Bridget. 'How mass atrocities end: an evidence-based counter-narrative', *Fletcher Forum of World Affairs*, Vol. 36, No. 1, Winter 2012, pp. 15–31.
Nambiar, Vijay. 'The protection of civilians and the United Nations', *Strategic Analysis*, Vol. 35, No. 6, November 2011, pp. 921–926.

Conflict, violence, and security – books

Battistella, Dario. *Paix et guerres au XXIe siècle*. Auxerre: Sciences Humaines, 2011, 159 pp.
Coutau-Bégarie, Hervé. *Traité de stratégie*. 7e éd. revue et augm. Paris: Economica; Institut de stratégie et des conflits, 2011, 1200 pp.
Doaré, Ronan and Hude, Henri (dir.). *Les robots au coeur du champ de bataille: rencontres sur le thème de la robotisation du champ de bataille: aspects éthiques et juridiques*. Paris: Economica, 2011, 214 pp.
Dunigan, Molly. *Victory for hire: private security companies' impact on military effectiveness*. Stanford, CA: Stanford University Press, 2011, 235 pp.
Gardner, Hall and Kobtzeff, Oleg (eds). *The Ashgate research companion to war: origins and prevention*. Farnham and Burlington, VA: Ashgate, 2012, 664 pp.
Lee, Steven P. *Ethics and war: an introduction*. Cambridge: Cambridge University Press, 2012, 328 pp.
Lindley-French, Julian and Boyer, Yves (eds). *The Oxford handbook of war*. Oxford: Oxford University Press, 2012, 709 pp.
Odello, Marco and Beruto, Gian Luca (eds). *Global violence: consequences and responses*. Milan: Franco Angeli; International Institute of Humanitarian Law, 2011, 224 pp.
Sloan, Elinor C. *Modern military strategy: an introduction*. Abingdon and New York: Routledge, 2012, 151 pp.
Snyder, Craig A. (ed.). *Contemporary security and strategy*, 3rd edn. Basingstoke and New York: Palgrave Macmillan, 2012, 372 pp.
Trevett, Michael F. *Isolating the guerrilla*. Mustang, OK: Tate, 2011, 474 pp.

Conflict, violence, and security – articles

Klein, Josh and Lavery, Cathy. 'Legitimating war by victimization: state-corporate crime and public opinion', *Crime, Law and Social Change*, Vol. 56, No. 3, October 2011, pp. 301–316.
Kunkeler, Josjah and Peters, Krijn. '"The boys are coming to town": youth, armed conflict and urban violence in developing countries', *International Journal of Conflict and Violence*, Vol. 5, No. 2, 2011, pp. 277–291.
O'Brien, Thomas. 'Food riots as representations of insecurity: examining the relationship between contentious politics and human security', *Conflict, Security, and Development*, Vol. 12, No. 1, March 2012, pp. 31–49.
Rid, Thomas. 'Cyber war will not take place', *Journal of Strategic Studies*, Vol. 35, No. 1, February 2012, pp. 5–32.
Watts, Michael J. 'Economies of violence: reflections on the World Development Report 2011', *Humanity: An International Journal of Human Rights, Humanitarianism, and Development*, Vol. 3, No. 1, Spring 2012, pp. 115–130.

Zubair Shah, Pir *et al.* 'Obama's secret wars', *Foreign Policy*, No. 192, March/April 2012, pp. 56–96.

Detention – books

Gross, Hyman Gross. *Crime and punishment: a concise moral critique*. Oxford: Oxford University Press, 2012, 219 pp.
Human Rights Watch. *Old behind bars: the aging prison population in the United States*. New York: Human Rights Watch, 2012, 104 pp.
Humbert, Sylvie, Derasse, Nicolas, et Royer, Jean-Pierre (sous la dir. de). *La prison, du temps passé au temps dépassé*. Paris: L'Harmattan, 2012, 230 pp.
Meneghetti, Francesca. *Di là del muro: il campo di concentramento di Treviso (1942–1943)*. Treviso: ISTRESCO, 2012, 503 pp.
Observatoire international des prisons. *Les conditions de détention en France: rapport 2011*. Paris: La Découverte, 2012, 336 pp.
Snacken, Sonja. *Prisons en Europe: pour une pénologie critique et humaniste*. Bruxelles: Larcier, 2011, 249 pp.
Sun, Jian and Masipag, Miguel (eds). *Terrorists, enemy combatant detainees and the judicial system*. New York: Nova Science, 2011, 156 pp.

Detention – articles

Blank, Laurie R. 'A square peg in a round hole: stretching law of war detention too far', *Rutgers Law Review*, Vol. 63, No. 4, Summer 2011, pp. 1169–1193.
Buys, Cindy G. 'Nottebohm's nightmare: have we exorcised the ghosts of WWII detention programs or do they still haunt Guantanamo?', *Chicago-Kent Journal of International and Comparative Law*, Vol. 11, 2011, pp. 1–77.
de Londras, Fiona. 'Can counter-terrorist internment ever be legitimate?', *Human Rights Quarterly: A Comparative and International Journal of the Social Sciences, Humanities, and Law*, Vol. 33, No. 3, August 2011, pp. 593–619.
Frakt, David J. R. 'Mohammed Jawad and the military commissions of Guantánamo', *Duke Law Journal*, Vol. 60, issue 6, 2011, pp. 1367–1411.
Roeder, Tina. '"Schalit wird nicht der letzte sein": Geiselnahmen israelischer Soldaten durch militante arabische und palästinensische Gruppen', *Humanitäres Völkerrecht: Informationsschriften = Journal of International Law of Peace and Armed Conflict*, Vol. 25, No. 1, 2012, pp. 19–26.
Sassòli, Marco and Tougas, Marie-Louise. 'International law issues raised by the transfer of detainees by Canadian forces in Afghanistan', *McGill Law Journal = Revue de droit McGill*, Vol. 56, No. 4, June 2011, pp. 959–1010.
Walen, Alec. 'Transcending, but not abandoning the combatant–civilian distinction: a case study', *Rutgers Law Review*, Vol. 63, No. 4, Summer 2011, pp. 1149–1168.

Economy – books

Mehta, Vijay. *The economics of killing: how the West fuels war and poverty in the developing world*. London: Pluto Press, 2012, 237 pp.
Paillard, Christophe-Alexandre. *Les nouvelles guerres économiques: 110 fiches réponses aux questions clefs*. Paris: Ophrys, 2011, 633 pp.

Environment – books

Ferris, Elizabeth and Petz, Daniel. *The year that shook the rich: a review of natural disasters in 2011*. Washington, DC: Brookings Institution; London: London School of Economics Project on Internal Displacement, 2012, 142 pp.
Welzer, Harald Welzer; transl. by Patrick Camiller. *Climate wars: why people will be killed in the twenty-first century*. Cambridge and Malden, MA: Polity, 2012, 222 pp.

Geopolitics – books

Aitken, Jonathan. *Kazakhstan: surprises and stereotypes after 20 years of independence*. London and New York: Continuum, 2012, 200 pp.
Auroi, Claude and Helg, Aline (eds). *Latin America 1810–2010: dreams and legacies*. London: Imperial College Press, 2012, 538 pp.
Bravin, Hélène. *Kadhafi: vie et mort d'un dictateur*. Paris: F. Bourin, 2012, 265 pp.
Brehony, Noel. *Yemen divided: the story of a failed state in South Arabia*. London and New York: I. B. Tauris, 2011, 257 pp.
Bruneau, Thomas, Dammert, Lucía, and Skinner, Elizabeth (eds). *Maras: gang violence and security in Central America*. Austin, TX: University of Texas Press, 2011, 309 pp.
Carranca, Adriana. *O Afeganistão depois do talibã: onze histórias afegãs do 11 de Setembro e a década do terror*. Rio de Janeiro: Civilização Brasileira, 2011, 286 pp.
Council of Europe, Commissioner for Human Rights. *Post-war justice and durable peace in the former Yugoslavia*. Strasbourg: Council of Europe, 2012, 48 pp.
Delisle, Guy. *Chroniques de Jérusalem* (bande dessinée). [s.l.]: Guy Delcourt, 2011, 333 pp.
Harper, Mary. *Getting Somalia wrong? Faith, war and hope in a shattered state*. London and New York: Zed Books, 2012, 217 pp.
Larkin, Craig. *Memory and conflict in Lebanon: remembering and forgetting the past*. London and New York: Routledge, 2012, 226 pp.
Pollack, Kenneth M. *et al. The Arab awakening: America and the transformation of the Middle East*. Washington, DC: Brookings Institution, 2011, 381 pp.
Reno, William. *Warfare in independent Africa*. Cambridge: Cambridge University Press, 2011, 271 pp.
Vincent, Léonard. *Les Érythréens: récit*. Paris: Payot & Rivages, 2012, 245 pp.

Geopolitics – articles

Cotte Poveda, Alexander. 'Economic development, inequality and poverty: an analysis of urban violence in Colombia', *Oxford Development Studies*, Vol. 39, No. 4, December 2011, pp. 453–468.
Dalacoura, Katerina. 'The 2011 uprisings in the Arab Middle East: political change and geopolitical implications', *International Affairs*, Vol. 88, No. 1, January 2012, pp. 63–79.
Lefebvre, Michel *et al.* 'Guerre d'Algérie: mémoires parallèles', *Le Monde Hors-série*, février–mars 2012, 98 pp.
Sur, Serge *et al.* 'Printemps arabe et démocratie', *Questions internationales*, No. 53, janvier–février 2012, pp. 4–84.
Valencia Gutiérrez, Alberto (coord.). 'La Colombie', *Problèmes d'Amérique latine*, No. 83, hiver 2011–2012, pp. 7–116.

Health/medicine – books

Rubenstein, Leonard S. *Protection of health care in armed and civil conflict: opportunities for breakthroughs*. Washington, DC: Center for Strategic and International Studies, 2012, 10 pp.
Tobin, John. *The right to health in international law*. Oxford: Oxford University Press, 2012, 416 pp.

History – books

Douglas, R. M.; aus dem Englischen übersetzt von Martin Richter. *Ordnungsgemässe Ueberführung: die Vertreibung der Deutschen nach dem Zweiten Weltkrieg*. München, Berlin: C. H. Beck, 2012, 556 pp.
Pellissier, Pierre. *Solférino: 24 juin 1859*. [Paris]: Perrin, 2012, 218 pp.

Human rights – books

Human Rights Watch. *Human Rights Watch world report 2012: events of 2011*. New York: Human Rights Watch, 2012, 676 pp.

Human rights – articles

Greenwood, Christopher. 'Human rights and humanitarian law: conflict or convergence', *Case Western Reserve Journal of International Law*, Vol. 43, Nos. 1&2, 2010, pp. 491–512.

Padmanabhan, Vijay M. 'To transfer or not to transfer: identifying and protecting relevant human rights interests in non-refoulement', *Fordham Law Review*, Vol. 80, No. 1, October 2011, pp. 73–123.

Humanitarian aid – books

Al-Yahya, Khalid and Fustier, Nathalie. *Saudi Arabia as a humanitarian donor: high potential, little institutionalization*. Berlin: Global Public Policy Institute, 2011, 35 pp.
Barrett, Christopher B., Binder, Andrea, and Steets, Julia. *Uniting on food assistance: the case for transatlantic cooperation*. London and New York: Routledge, 2012, 157 pp.
DARA. *The humanitarian response index 2011: addressing the gender challenge*. Madrid: DARA, 2011, 329 pp.
Diplomatie humanitaire et gestion des crises internationales: actes de la conférence internationale organisée par la Fondation française de l'Ordre de Malte, 27–28 janvier 2011 à l'UNESCO. Saint-Évarzec: Editions du Palémon, 2012, 198 pp.
Glaser, Max P. *Engaging private security providers: a guideline for non-governmental organisations*. London: European Interagency Security Forum, 2011, 29 pp.
Hodge, Nathan. *Armed humanitarians: the rise of the nation builders*. New York: Bloomsbury, 2011, 338 pp.
Kondo Rossier, Masayo. *A review of practices and expert opinions: linking humanitarian action and peacebuilding*. Geneva: Graduate Institute of International and Development Studies–CCDP, 2011, 87 pp.
Magone, Claire, Neuman, Michael, and Weissman, Fabrice (eds). *Humanitarian negotiations revealed: the MSF experience*. New York: Columbia University Press; Médecins sans Frontières, 2011, 287 pp.
Meier, Claudia and Murthy, C. S. R. *India's growing involvement in humanitarian assistance*. Berlin: Global Public Policy Institute, 2011, 47 pp.
Nutt, Samantha. *Damned nations: greed, guns, armies and aid*. Toronto: Signal; McClelland and Stewart, 2011, 228 pp.
Okeke, Jide. *Why humanitarian aid in Darfur is not a practice of the 'responsibility to protect'*. Uppsala: Nordiska Afrikainstitutet, 2011, 45 pp.
South, Ashley *et al. Local to global protection in Myanmar (Burma), Sudan, South Sudan and Zimbabwe*. London: Overseas Development Institute, February 2012, 27 pp.
Zicherman, Nona *et al. Applying conflict sensitivity in emergency response: current practice and ways forward*. London: Overseas Development Institute, October 2011, 22 pp.

Humanitarian aid – articles

Audet, François. 'L'acteur humanitaire en crise existentielle: les défis du nouvel espace humanitaire', *Études internationales*, Vol. 42, No. 4, décembre 2011, pp. 447–472.
Cullen Dunn, Elizabeth. 'The chaos of humanitarian aid: adhocracy in the Republic of Georgia', *Humanity: An International Journal of Human Rights, Humanitarianism, and Development*, Vol. 3, No. 1, Spring 2012, pp. 1–23.
Guilhot, Nicolas. 'The anthropologist as witness: humanitarianism between ethnography and critique', *Humanity: An International Journal of Human Rights, Humanitarianism, and Development*, Vol. 3, No. 1, Spring 2012, pp. 81–101.
Joachim, Jutta and Schneiker, Andrea. 'New humanitarians? Frame appropriation through private military and security companies', *Millennium: Journal of International Studies*, Vol. 40, No. 2, 2012, pp. 365–388.
Knox-Clarke, Paul *et al.* 'Humanitarian accountability', *Humanitarian Exchange: The Magazine of the Humanitarian Practice Network*, No. 52, October 2011, 47 pp.
Kruke, Bjørn Ivar and Olsen, Odd Einar. 'Knowledge creation and reliable decision-making in complex emergencies', *Disasters: The Journal of Disaster Studies and Management*, Vol. 36, No. 2, April 2012, pp. 212–232.
Muggah, Robert with Kevin Savage. 'Urban violence and humanitarian action: engaging the fragile city', *Journal of Humanitarian Assistance*, 19 January 2012, 13 pp.
Orchard, Phil. 'The evolution of the responsibility to protect: at a crossroads?', *International Affairs*, Vol. 88, No. 2, March 2012, pp. 377–386.
Reinhardt, Dieter. 'Internationale humanitäre Hilfe zum Überleben: zwischen völkerrechtlicher Verpflichtung, nationalstaatlichen Interessen und Spendenmarkt', *Internationale Politik und Gesellschaft*, No. 4, 2011, pp. 151–161.
Weber, Romana. 'Is there a right of human rights organizations to protect their sources?', *Schweizerische Zeitschrift für internationales und europäisches Recht = Revue suisse de droit international et de droit européen = Rivista svizzera di diritto internazionale e europeo = Swiss Review of International and European Law*, 21e année, No. 4, 2011, pp. 669–678.

ICRC/International Movement of the Red Cross and Red Crescent – books

Vanni, Paolo; présentation Jakob Kellenberger, Francesco Rocca; préf. Francesco Caponi. *Algérie, grands hommes oubliés: siège de Paris 1870: manuscrits de Henry Dunant 4576–4593* (film n. 817 – CD F1719). Firenze: Croce Rossa Italiana, 2011, 2 vols, 692 pp.

ICRC/International Movement of the Red Cross and Red Crescent – articles

Bugnion, François. 'Confronting the unthinkable: the International Committee of the Red Cross and the Cuban missile crisis, October–November 1962 (Part One)', *Schweizerische Zeitschrift für Geschichte = Revue suisse d'histoire = Rivista storica svizzera*, Vol. 62, No. 1, 2012, pp. 143–155.
La Porte, Pablo. 'Víctimas del Rif (1921–1926): memoria, acción humanitaria y lecciones para nuestro tiempo', *Revista de estudios internacionales mediterráneos*, Núm. 10, enero–junio 2011, pp. 116–133.

International criminal law – books

Bornkamm, Paul Christoph. *Rwanda's Gacaca courts: between retribution and reparation*. Oxford: Oxford University Press, 2012, 242 pp.
Bosly, Henri D. and Vandermeersch, Damien. *Génocide, crimes contre l'humanité et crimes de guerre face à la justice: les juridictions internationales et les tribunaux nationaux*, 2ème éd. Bruxelles: Bruylant, 2012, 285 pp.
Giorgetti, Chiara. *The rules, practice, and jurisprudence of international courts and tribunals*. Leiden and Boston, MA: M. Nijhoff, 2012, 611 pp.
Horvitz, Leslie Alan and Catherwood, Christopher. *Encyclopedia of war crimes and genocide*, rev. edn. New York: Facts on File, 2011, 2 vols, 694 pp.
Olasolo, Hector. *Essays on international criminal justice*. Oxford and Portland, OR: Hart, 2012, 213 pp.
Schabas, William A. *An introduction to the International Criminal Court*, 4th edn. Cambridge: Cambridge University Press, 2011, 579 pp.
Wolf, Willem-Jan van der (ed.). *War crimes and international criminal law*. The Hague: International Courts Association, 2011, 641 pp.

International criminal law – articles

Badescu, Valentin Stelian. 'Short considerations on the international criminal liability in the context of armed conflict in the contemporary period', *Studii de drept romanesc = Romanian Law Studies Review*, Year 23, Vol. 56, No. 2, April–June 2011, pp. 187–202.
Bashi, J. Solomon. 'Prosecuting starvation in the Extraordinary Chambers in the Courts of Cambodia', *Wisconsin International Law Journal*, Vol. 29, Spring 2011, pp. 34–69.
Haque, Adil Ahmad. 'Protecting and respecting civilians: correcting the substantive and structural defects of the Rome Statute', *New Criminal Law Review*, Vol. 14, No. 4, Fall 2011, pp. 519–575.
Kress, Claus and Webb, Philippa (eds). 'Aggression: after Kampala', *Journal of International Criminal Justice*, Vol. 10, No. 1, March 2012, 288 pp.

Streichler, Stuart. 'The war crimes trial that never was: an inquiry into the war on terrorism, the laws of war, and presidential accountability', *University of San Francisco Law Review*, Vol. 45, No. 4, Spring 2011, pp. 959–1004.
Swart, Mia. 'Tadic revisited: some critical comments on the legacy and the legitimacy of the ICTY', *Goettingen Journal of International Law*, Vol. 3, No. 3, 2011, pp. 985–1009.

International humanitarian law: generalities – books

Documentos oficiales: conferencia diplomática sobre la adopción del tercer Protocolo adicional a los Convenios de Ginebra relativo a la aprobación de un signo distintivo adicional (Protocolo III), 5–8 de diciembre de 2005, Ginebra, Suiza / Confédération Suisse, Departamento Federal de Asuntos Exteriores DFAE. Berna: Departamento Federal de Asuntos Exteriores, 2012, 133 pp.
Documents officiels: conférence diplomatique sur l'adoption du troisième Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à l'adoption d'un signe distinctif additionnel (Protocole III), 5–8 décembre 2005, Genève, Suisse / Confédération Suisse, Département fédéral des affaires étrangères DFAE. Berne: Département fédéral des affaires étrangères, 2012, 134 pp.
Gasser, Hans-Peter und Melzer, Nils; mit einer Einleitung von Daniel Thürer. *Humanitäres Völkerrecht: eine Einführung*, 2. überarbeitete Aufl. Genf: Schulthess; Baden-Baden: NOMOS, 2012, 280 pp.
Margulies, Peter. *The fog of war reform: change and structure in the law of armed conflict after September 11*. [Bristol, RI]: Roger Williams University School of Law, 2011, 47 pp.
Official documents: diplomatic conference on the adoption of a third Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the adoption of an additional distinctive emblem (Protocol III), 5–8 December 2005, Geneva, Switzerland / Confédération Suisse, Federal Department of Foreign Affairs FDFA. Bern: Federal Department of Foreign Affairs, 2012, 132 pp.
Perrin, Benjamin (ed.). *Modern warfare: Armed groups, private militaries, humanitarian organizations, and the law*. Vancouver: UBC Press, 2012, 420 pp.
Van Schaack, Beth. *IHL supplement for use in courses in international criminal law*. [Santa Clara, CA]: Santa Clara University School of Law, March 2012, 52 pp.

International humanitarian law: generalities – articles

Blank, Laurie R. 'A new twist on an old story: lawfare and the mixing of proportionalities', *Case Western Reserve Journal of International Law*, Vol. 43, No. 3, 2011, pp. 707–738.
Borrmann, Robin and Heintze, Hans-Joachim. 'XXXIV. round table on current issues of international humanitarian law: international humanitarian law and new weapons technologies: San Remo, 8. bis 10. September 2011', *Humanitäres*

Völkerrecht: Informationsschriften = Journal of International Law of Peace and Armed Conflict, Vol. 24, No. 4, 2011, pp. 216–219.
Lucas, George R. '"New rules for new wars": international law and just war doctrine for irregular war', *Case Western Reserve Journal of International Law*, Vol. 43, No. 3, 2011, pp. 677–705.
Mégret, Frédéric. 'War and the vanishing battlefield', *Loyola University Chicago International Law Review*, Vol. 9, No. 1, Fall/Winter 2011, pp. 131–155.
Okimoto, Keiichiro. 'The cumulative requirements of *jus ad bellum* and *jus in bello* in the context of self-defense', *Chinese Journal of International Law*, Vol. 11, No. 1, March 2012, pp. 45–75.
Stürchler, Nikolas. 'Der Begriff des Krieges im Völkerrecht: spezifisch unter dem Gesichtspunkt des Neutralitätsrechts', *Schweizerische Zeitschrift für internationales und europäisches Recht = Revue suisse de droit international et de droit européen = Rivista svizzera di diritto internazionale e europeo = Swiss Review of International and European Law*, 21e année, No. 4, 2011, pp. 627–645.
Talbot Jensen, Eric. 'Applying a sovereign agency theory of the law of armed conflict', *Chicago Journal of International Law*, Vol. 12, Winter 2012, pp. 685–727.

International humanitarian law: conduct of hostilities – books

Blank, Laurie R. *Military operations, battlefield reality and the judgment's impact on effective implementation and enforcement of international humanitarian law*. Atlanta, GA: International Humanitarian Law Clinic at Emory University School of Law, 2012, 17 pp.
Finkelstein, Claire, Ohlin, Jens David, and Altman, Andrew (eds). *Targeted killings: law and morality in an asymmetrical world*. Oxford: Oxford University Press, 2012, 496 pp.
Michael N. Schmitt. *Essays on law and war at the fault lines*. The Hague: T. M. C. Asser Press; Berlin and Heidelberg: Springer, 2012, 637 pp.

International humanitarian law: conduct of hostilities – articles

Blank, Laurie R. 'After "Top Gun": how drone strikes impact the law of war', *University of Pennsylvania Journal of International Law*, Vol. 33, No. 3, Spring 2012, pp. 675–718.
Corn, Geoffrey and Jenks, Chris. 'Two sides of the combatant coin: untangling direct participation in hostilities from belligerent status in non-international armed conflicts', *University of Pennsylvania Journal of International Law*, Vol. 33, No. 2, Winter 2011, pp. 313–362.
Fellmeth, Aaron. 'The proportionality principle in operation: methodological limitations of empirical research and the need for transparency', *Israel Law Review*, Vol. 45, No. 1, 2012, pp. 125–150.

Geiss, Robin. 'The principle of proportionality: "force protection" as a military advantage', *Israel Law Review*, Vol. 45, No. 1, 2012, pp. 71–89.
Kessler, Joshua L. 'The Goldstone Report: politicization of the law of armed conflict and those left behind', *Military Law Review*, Vol. 209, Fall 2011, pp. 69–121.
Kleffner, Jann K. 'Section IX of the ICRC interpretive guidance on direct participation in hostilities: the end of *jus in bello* proportionality as we know it?', *Israel Law Review*, Vol. 45, No. 1, 2012, pp. 35–52.
Kreps, Sarah and Kaag, John. 'The use of unmanned aerial vehicles in contemporary conflict: a legal and ethical analysis', *Polity Advance Online Publication*, 13 February 2012, 26 pp.
Radsan, Afsheen John and Murphy, Richard. 'Measure twice, shoot once: higher care for CIA-targeted killing', *University of Illinois Law Review*, Vol. 2011, No. 4, pp. 1201–1241.
van Steenberghe, Raphaël. 'Proportionality under *jus ad bellum* and *jus in bello*: clarifying their relationship', *Israel Law Review*, Vol. 45, No. 1, 2012, pp. 107–124.
Ziegler, Reuven (Ruvi) and Otzari, Shai. 'Do soldiers' lives matter? A view from proportionality', *Israel Law Review*, Vol. 45, No. 1, 2012, pp. 53–69.

International humanitarian law: implementation – books

Wilkinson, Stephen. *Standards of proof in international humanitarian and human rights fact-finding and inquiry missions*. Geneva: Geneva Academy of International Humanitarian Law and Human Rights, 2011, 69 pp.

International humanitarian law: implementation – articles

Blank, Laurie R. 'Understanding when and how domestic courts apply IHL', *Case Western Reserve Journal of International Law*, Vol. 44, 2011, 20 pp.
Krajewski, Markus. 'Schadensersatz wegen Verletzungen des Gewaltverbots als ius post bellum am Beispiel der Eritrea-Ethiopia Claims Commission', *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht = Heidelberg Journal of International Law*, 72. Jg., No. 1, 2012, pp. 147–176.

International humanitarian law: law of occupation – books

Benvenisti, Eyal. *The international law of occupation*, 2nd edn. Oxford: Oxford University Press, 2012, 383 pp.

International humanitarian law: law of occupation – articles

Benoliel, Daniel. 'Israel, Turkey, and the Gaza blockade', *University of Pennsylvania Journal of International Law*, Vol. 33, No. 2, Winter 2011, pp. 615–662.
Kashgar, Maral. 'The ECtHR's judgment in Al-Jedda and its implications for international humanitarian law', *Humanitäres Völkerrecht: Informationsschriften = Journal of International Law of Peace and Armed Conflict*, Vol. 24, No. 4, 2011, pp. 229–233.
Stein, Jeffrey D. 'Waging waterfare: Israel, Palestinians, and the need for a new hydro-logic to govern water rights under occupation', *New York Journal of International Law and Politics*, Vol. 44, No. 1, Fall 2011, pp. 165–217.

International humanitarian law: types of actor – books

Bakker, Christine and Sossai, Mirko (eds). *Multilevel regulation of military and security contractors: the interplay between international, European and domestic norms*. Oxford and Portland, OR: Hart, 2012, 625 pp.
Minear, Larry. *Through veteran's eyes: the Iraq and Afghanistan experience*. Dulles, VA: Potomac Books Inc., 2010, 243 pp.

International humanitarian law: types of actor – articles

Bosch, S. and Maritz, M. 'South African private security contractors active in armed conflicts: citizenship, prosecution and the right to work', *Potchefstroom Electronic Law Journal*, Vol. 14, No. 7, 2011, pp. 71–125.
Buckley, Orla Marie. 'Unregulated armed conflict: non-state armed groups, international humanitarian law, and violence in Western Sahara', *North Carolina Journal of International Law and Commercial Regulation*, Vol. 37, Spring 2012, pp. 793–845.
Chang, Karl S. 'Enemy status and military detention in the war against al-Qaeda', *Texas International Law Journal*, Vol. 47, No. 1, 2011, pp. 1–73.
Hansen, Joseph C. 'Rethinking the regulation of private military and security companies under international humanitarian law', *Fordham International Law Journal*, Vol. 35, No. 3, 2011, pp. 698–736.
Heller, Kevin Jon. 'The law of neutrality does not apply to the conflict with Al-Qaeda, and it's a good thing, too: a response to Chang', *Texas International Law Journal*, Vol. 47, No. 1, Fall 2011, pp. 115–141.
Ingber, Rebecca. 'Untangling belligerency from neutrality in the conflict with Al-Qaeda', *Texas International Law Journal*, Vol. 47, No. 1, Fall 2011, pp. 75–114.
Krahmann, Elke. 'From "mercenaries" to "private security contractors": the (re) construction of armed security providers in international legal discourses', *Millennium Journal of International Studies*, Vol. 40, No. 2, 2012, pp. 343–363.

Richemond-Barak, Daphne. 'Applicability and application of the laws of war to modern conflicts', *Florida Journal of International Law*, Vol. 23, No. 3, December 2011, pp. 327–357.
Roberts, Anthea and Sivakumaran, Sandesh. 'Lawmaking by nonstate actors: engaging armed groups in the creation of international humanitarian law', *Yale Journal of International Law*, Vol. 37, issue 1, 2012, pp. 107–152.
Ryngaert, Cedric and van de Meulebroucke, Anneleen. 'Enhancing and enforcing compliance with international humanitarian law by non-state armed groups: an inquiry into some mechanisms', *Journal of Conflict and Security Law*, Vol. 16, No. 3, Winter 2011, pp. 443–472.

International humanitarian law: types of conflict – books

Ford, Christopher A. and Cohen, Amichai. *Rethinking the law of armed conflict in an age of terrorism*. Lanham, MD: Lexington Books, 2012, 325 pp.
Crawford, Emily. *Virtual battlegrounds: direct participation in cyber warfare*. [Sydney]: University of Sydney Law School, 2012, 20 pp.

International humanitarian law: types of conflict – articles

Estreicher, Samuel. 'Privileging asymmetric warfare (part III)? The intentional killing of civilians under international humanitarian law', *Chicago Journal of International Law*, Vol. 12, Winter 2012, pp. 589–603.
Otálora Lozano, Guillermo and Machado, Sebastián. 'The objective qualification of non-international armed conflicts: a Colombian case study', *Amsterdam Law Forum*, Vol. 4, No. 1, Winter 2012, pp. 58–77.
Peterke, Sven. 'Völkerrechtliches Selbstverteidigungsrecht gegen transnationales organisiertes Verbrechen?', *Humanitäres Völkerrecht: Informationsschriften = Journal of International Law of Peace and Armed Conflict*, Vol. 24, No. 4, 2011, pp. 202–215.
Singh, Oinam Jitendra. 'Armed violence in Manipur and human rights', *Indian Journal of Political Science*, Vol. 72, No. 4, October–December 2011, pp. 997–1006.
Talbot Jensen, Eric. 'Sovereignty and neutrality in cyber conflict', *Fordham International Law Journal*, Vol. 35, No. 3, 2012, pp. 815–841.

Media – books

Freedman, Des and Kishan Thussu, Daya (eds). *Media and terrorism: global perspectives*. London: Sage, 2012, 322 pp.
Karatzogianni, Athina (ed.). *Violence and war in culture and the media: five disciplinary lenses*. London and New York: Routledge, 2012, 280 pp.
Simon, Joel *et al.*; pref. by Sandra Mims Rowe. *Attacks on the press in 2011: a worldwide survey by the Committee to Protect Journalists*. New York: Committee to Protect Journalists, 2012, 451 pp.

Peace – books

Arcidiacono, Bruno. *Cinq types de paix: une histoire des plans de pacification perpétuelle (XVIIe–XXe siècles)*. Paris: Presses universitaires de France, 2011, 465 pp.
Devin, Guillaume; transl. by Roger Leverdier. *Making peace: the contribution of international institutions*. Basingstoke and New York: Palgrave Macmillan, 2011, 192 pp.
von Hehn, Arist; with a foreword by Martti Ahtisaari. *The internal implementation of peace agreements after violent intrastate conflict: guidance for internal actors responsible for implementation*. Leiden and Boston, MA: M. Nijhoff, 2011, 448 pp.

Psychology – books

Comoretto, Amanda, Crichton, Nicola, and Albery, Ian. *Resilience in humanitarian aid workers: understanding processes of development*. Saarbrücken: Lambert Academic Publishing, 2011, 359 pp.
World Health Organization, War Trauma Foundation, and World Vision International. *Psychological first aid: guide for field workers*. Geneva: WHO, 2011, 60 pp.

Psychology – articles

Shaley, Ronit and Ben-Asher, Smadar. 'Ambiguous loss: the long-term effects on the children of POWs', *Journal of Loss and Trauma*, Vol. 16, issue 6, 2011, pp. 511–528.

Public international law – books

Benatar, Marco and Gombeer, Kristof. *Cyber sanctions: exploring a blind spot in the current legal debate*. [s.l.]: European Society of International Law, 2011, 23 pp.
Dinstein, Yoram. *War, aggression and self-defence*. 5th edn. Cambridge: Cambridge University Press, 2011, 375 pp.
Eckart, Christian. *Promises of states under international law*. Oxford and Portland, OR: Hart, 2012, 335 pp.

Public international law – articles

Brilmayer, Lea and Yemane Tesfalidet, Isaias. 'Third state obligations and the enforcement of international law', *New York University Journal of International Law and Politics*, Vol. 44, No. 1, Fall 2011, pp. 1–53.

Brilmayer, Lea and Yemane Tesfalidet, Isaias. 'Treaty denunciation and "withdrawal" from customary international law: an erroneous analogy with dangerous consequences', *Yale Law Journal Online*, Vol. 120, 2011, pp. 217–231.
Schmitt, Michael N. 'Cyber operations and the *jus ad bellum* revisited', *Villanova Law Review*, Vol. 56, No. 3, 2011, pp. 569–605.
Simm, Gabrielle. 'International law as a regulatory framework for sexual crimes committed by peacekeepers', *Journal of Conflict and Security Law*, Vol. 16, No. 3, Winter 2011, pp. 473–506.
Vázquez, Carlos M.. 'Withdrawing from international custom: terrible food, small portions', *Yale Law Journal Online*, Vol. 120, 2011, pp. 269–291.

Refugees/displaced persons – books

Gureyeva-Aliyeva, Yulia and Huseynov, Tabib. *'Can you be an IDP for twenty years?' A comparative field study on the protection needs and attitudes towards displacement among IDPs and host communities in Azerbaijan*, Baku: Brookings Institution and London School of Economics Project on Internal Displacement, 2011, 48 pp.
Markard, Nora. *Kriegsflüchtlinge: Gewalt gegen Zivilpersonen in bewaffneten Konflikten als Herausforderung für das Flüchtlingsrecht und den subsidiären Schutz*. Tübingen: Mohr Siebeck, 2012, 413 pp.
McAdam, Jane. *Climate change, forced migration, and international law*. Oxford: Oxford University Press, 2012, 319 pp.
Schnieper, Marlène. *Nakba: die offene Wunde: die Vertreibung der Palästinenser 1948 und die Folgen*. Zürich: Rotpunktverlag, 2012, 380 pp.
Vieira Sanches, Charles L. *Migrations internationales et droits de l'homme: approche systémique sur les protections accordées aux migrants*. Saarbrücken: Éditions universitaires européennes, 2011, 119 pp.

Refugees/displaced persons – articles

Syring, Tom. 'Beyond occupation: protected persons and the expiration of obligations', *ILSA Journal of International and Comparative Law*, Vol. 17, No. 2, Spring 2011, pp. 417–435.
Churruca Muguruza, Cristina. 'La protección y búsqueda de soluciones duraderas para las personas desplazadas internamente', *Anuario de acción humanitaria y derechos humanos = Yearbook on Humanitarian Action and Human Rights*, No. 9, 2011, pp. 15–28.

Religion – books

Amir-Aslani, Ardavan. *La guerre des dieux: géopolitique de la spiritualité*. Paris: Nouveau Monde, 2011, 319 pp.

Constanta Ciolac, Adina. *Qu'est-ce qu'un conflit religieux? Une approche systématique du lien entre la religion et la violence à travers l'histoire*. Genève: [s.n.], 2011, 367 pp.
Witte, John and Green, M. Christian (eds). *Religion and human rights: an introduction*. Oxford: Oxford University Press, 2012, 392 pp.

Religion – articles

Basedau, Matthias *et al.* 'Do religious factors impact armed conflict? Empirical evidence from Sub-Saharan Africa', *Terrorism and Political Violence*, Vol. 23, No. 5, 2011, pp. 752–779.
Mason, Simon J. A. *et al.* 'Religion in conflict transformation', *Politorbis: revue de politique étrangère*, No. 52, 2/2011, 105 pp.

Terrorism – books

Kaveh le forgeron. *Le Hezbollah global: les réseaux secrets de l'Iran*. Paris: Choiseul, 2012, 378 pp.
Pantuliano, Sara *et al. Counter-terrorism and humanitarian action: tensions, impact and ways forward*. London: Humanitarian Policy Group, Overseas Development Institute, October 2011, 12 pp.
Rabino, Thomas. *De la guerre en Amérique: essai sur la culture de guerre*. [Paris]: Perrin, 2011, 535 pp.
Salinas de Frías, Ana María, Samuel, Katja L. H., and White, Nigel D. (eds). *Counter-terrorism: international law and practice*. Oxford: Oxford University Press, 2012, 1156 pp.

Terrorism – articles

Sabel, Robbie. 'The legality and reciprocity of the war against terrorism', *Case Western Reserve Journal of International Law*, Vol. 43, No. 1&2, 2011, pp. 473–482.
Tams, Christian J. and Devaney, James G. 'Applying necessity and proportionality to anti-terrorist self-defence', *Israel Law Review*, Vol. 45, No. 1, 2012, pp. 91–106.
Torres Soriano, Manuel R. 'The vulnerabilities of online terrorism', *Studies in Conflict and Terrorism*, Vol. 35, No. 4, 2012, pp. 263–277.

Torture – books

Allhoff, Fritz. *Terrorism, ticking time-bombs, and torture: a philosophical analysis*. Chicago, IL: University of Chicago Press, 2012, 266 pp.

Dewulf, Steven. *The signature of evil: (re)defining torture in international law*. Cambridge: Intersentia, 2011, 617 pp.
Juin, Claude. *Des soldats tortionnaires: guerre d'Algérie: des jeunes gens ordinaires confrontés à l'intolérable*. Paris: Robert Laffont, 2012, 363 pp.
Kamm, F. M. *Ethics for enemies: terror, torture, and war*. Oxford: Oxford University Press, 2011, 178 pp.
Kelly, Tobias. *This side of silence: human rights, torture, and the recognition of cruelty*. Philadelphia, PA: University of Pennsylvania Press, 2012, 220 pp.
Panh, Rithy avec Christophe Bataille. *L'élimination*. Paris: Grasset, 2011, 332 pp.
Peirce, Gareth. *Dispatches from the dark side: on torture and the death of justice*. London and New York: Verso, 2012, 140 pp.

Torture – articles

Hollyer, James R. and Rosendorff B. Peter. 'Why do authoritarian regimes sign the Convention against Torture? Signaling, domestic politics and non-compliance', *Quarterly Journal of Political Science*, Vol. 6, Nos. 3–4, 2011, pp. 275–327.

Women/gender – books

Cheldelin, Sandra I. and Eliatamby Maneshka (eds). *Women waging war and peace: international perspectives on women's roles in conflict and post-conflict reconstruction*. London and New York: Continuum, 2011, 305 pp.
Cubero, José. *La femme et le soldat: viols et violences de guerre du Moyen Âge à nos jours*. Paris: Imago, 2012, 355 pp.
Lagoutte, Stéphanie et Svaneberg, Nina (éds). *Les droits de la femme et de l'enfant: réflexions africaines = Women and children's rights: African views*. Paris: Karthala, 2011, 384 pp.
Rajan, V. G. Julie. *Women suicide bombers: narratives of violence*. Abingdon and New York: Routledge, 2011, 384 pp.
Sjoberg, Laura and Gentry, Caron E. (eds) *Women, gender, and terrorism*. Athens, GA and London: University of Georgia Press, 2011, 250 pp.
Skjelsbaek, Inger. *The political psychology of war rape: studies from Bosnia and Herzegovina*. London and New York: Routledge, 2012, 172 pp.

Women/gender – articles

Tabak, Shana. 'False dichotomies of transitional justice: gender, conflict and combatants in Colombia', *New York University Journal of International Law and Politics*, Vol. 44, No. 1, Fall 2011, pp. 103–163.

INTERNATIONAL REVIEW of the Red Cross

The Review is printed in English and is published four times a year, in Spring, Summer, Autumn and Winter.

Annual selections of articles are also published on a regional level in Arabic, Chinese, French, Russian and Spanish.

Published in association with Cambridge University Press.

Submission of manuscripts

The International Review of the Red Cross invites submissions of manuscripts on subjects relating to international humanitarian law, policy and action. Most issues focus on particular topics, decided by the Editorial Board, which can be consulted under the heading Future Themes on the website of the Review. Submissions related to these themes are particularly welcome.

Articles may be submitted in Arabic, Chinese, English, French, Russian and Spanish. Selected articles are translated into English if necessary.

Submissions must not have been published, submitted or accepted elsewhere. Articles are subjected to a peer-review process; the final decision on publication is taken by the Editor-in-Chief. The Review reserves the right to edit articles. Notification of acceptance, rejection or the need for revision will be given within four weeks of receipt of the manuscript. Manuscripts will not be returned to the authors.

Manuscripts may be sent by e-mail to:
review@icrc.org

Manuscript requirements
Articles should be 5,000 to 10,000 words in length. Shorter contributions can be published under the section Notes and comments.

For further information, please consult the Information for contributors and Guidelines for referencing on the website of the Review:
www.icrc.org/eng/resources/international-review.

Subscriptions

Requests for subscriptions can be made to the following address:

Cambridge University Press, The Edinburgh Building, Shaftesbury Road, Cambridge CB2 8RU; or in the USA, Canada and Mexico, email journals@cambridge.org: Cambridge University Press, 32 Avenue of the Americas, New York, NY 10013-2473, email journals_subscriptions@cup.org.

The subscription price which includes delivery by air where appropriate (but excluding VAT) of volume 94, 2012, which includes print and online access is £227.00 (US $432.00 in USA, Canada and Mexico) for institutions; £30.00 (US $57.00 in USA, Canada and Mexico) for individuals, which includes print only. Single parts are £62.00 (US $112.00 in USA, Canada and Mexico) plus postage. EU subscribers (outside the UK) who are not registered for VAT should add VAT at their country's rate. VAT registered members should provide their VAT registration number. Japanese prices for institutions (including ASP delivery) are available from Kinokuniya Company Ltd, P.O. Box 55, Chitose, Tokyo 156, Japan.

Cover photo: Afghan residents look at a robot during a road clearance patrol in Logar province.
© Umit Bektas, Reuters

Photo research: Fania Khan Mohammad, ICRC

New technologies and warfare

Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

ICRC

ISSN 1816-3831

www.icrc.org/eng/resources/international-review

Cambridge Journals Online
For further information about this journal please go to the journal web site at:
http://www.journals.cambridge.org/irc

CAMBRIDGE UNIVERSITY PRESS