

International Institute of Humanitarian Law



International Institute of Humanitarian Law
Institut International de Droit Humanitaire
Istituto Internazionale di Diritto Umanitario

International Humanitarian Law and New Weapon Technologies

STUDI



Politica



FrancoAngeli

International Humanitarian Law and New Weapon Technologies

Although there can be no doubt that International Humanitarian Law applies to new weaponry and technological developments, subsuming a new technology under pre-existing rules always raises the question as to whether or not this is sufficient in terms of legal clarity, in view of the specific characteristics of new technology and – above all – the humanitarian impact such technology may have. The book comprises a series of contributions by prominent scholars, experts and practitioners from different countries who extensively explore the legal aspect of an array of new weapons and military technologies that have only recently entered the battlefield or that are now being tested with a view to being used for military purposes in the future. These not only include drones, robots and military outer space technologies but also cyber-technology and other devices and technologies, all of which raise important legal questions and humanitarian concerns.

The **International Institute of Humanitarian Law** is an independent, non-profit humanitarian organization founded in 1970. Its headquarters are situated in Villa Ormond, Sanremo (Italy). Its main objective is the promotion and dissemination of International Humanitarian Law, human rights, refugee law and migration law. Thanks to its longstanding experience and its internationally acknowledged academic standards, the International Institute of Humanitarian Law is considered to be a centre of excellence and has developed close co-operation with the most important international organizations.



International Institute of Humanitarian Law
Institut International de Droit Humanitaire
Istituto Internazionale di Diritto Umanitario

International Humanitarian Law and New Weapon Technologies

34th Round Table on Current Issues
of International Humanitarian Law
(Sanremo, 8th-10th September 2011)

Editor Wolff Heintschel von Heinegg

Associated Editor Gian Luca Beruto

 **FrancoAngeli**

Prof. Wolff Heintschel von Heinegg is professor of public international law at the Europa-Universität Viadrina, Frankfurt (Oder), Germany, where he also serves as the university's Vice-President. Professor Heintschel von Heinegg has been a member of the International Institute of Humanitarian Law's Council since 2007.

Mr. Gian Luca Beruto has a degree in International Political Science and is currently assistant to the Secretary-General of the International Institute of Humanitarian Law. In 2005 and 2006, he participated in a United Nations Peacekeeping mission in the Democratic Republic of Congo (MONUC) as part of the UN programme for disarmament.

The International Institute of Humanitarian Law would like to thank Mrs Shirley Morren, librarian of the Institute, who was both involved in the painstaking task of proof reading.

Copyright © 2012 by International Institute of Humanitarian Law

Stampa: Tipomozza, via Merano 18, Milano.

Table of Content

Acknowledgements	pag.	9
Preface		
<i>Fausto Pocar</i>	»	11
I. Opening session		
Opening remarks		
<i>Maurizio Moreno</i>	»	15
Welcome address		
<i>Giovanni Berrino</i>	»	21
Keynote address		
<i>Jakob Kellenberger</i>	»	23
Statement		
<i>Peter Maurer</i>	»	29
<i>Vincenzo Camporini</i>	»	33
<i>Betty E. King</i>	»	35
<i>Carmine De Pascale</i>	»	37
<i>Laura Mirachian</i>	»	41
<i>Francesco Rocca</i>	»	43

II. Legal and operational impact of technology on modern warfare

Setting the scene: new challenges for IHL <i>Michael Bothe</i>	pag.	51
New technologies: science fiction or real world? <i>Theresa Hitchens</i>	»	57
Impact on military strategy, capability development and doctrine <i>Erwin Dahinden</i>	»	64
New conflicts, new technologies: the challenge of the protection of the civilian population <i>Soad Shalaby</i>	»	74

III. Old weapons and new technologies. How new technologies enhance traditional weapons and weapon systems

Kinetic and non-kinetic energy weapons: a marriage made in heaven? <i>Stuart Casey-Maslen</i>	»	83
Satellite technology and humanitarian law <i>Joshua Cowan Lyons</i>	»	87

IV. Robots, remote-controlled and autonomous weapon systems

Ethics and artificial intelligence <i>Ronald Arkin</i>	»	95
Operational advantages and risks in the use of UAVs <i>Eugene Miasnikov</i>	»	104
Drones proliferation and protection of civilians <i>Noel Sharkey</i>	»	108
Autonomous systems: precautions in attacks <i>William H. Boothby</i>	»	119

Non-lethal capabilities – a double-edged sword
Richard Froh pag. 125

V. Cyber warfare

Operational reality of cyber warfare
Herb Lin » 137

Cyber warfare: is there a need for new law?
Matthew Waxman » 144

How to integrate cyber defence into existing defence capabilities
Suleyman Anil » 148

Humanitarian aspects of cyber warfare
Robin Geiss » 153

VI. New technologies: the way ahead

Law, technology and the conduct of hostilities in space
Michel Bourbonnière » 159

Law at cyberspeed: answering military cyber operators' legal questions
Gary Brown » 166

Towards a code of conduct for cyber space
Nils Melzer » 171

Discriminate, precise, proportional
Yedidia Yaari » 175

Concluding remarks
Philip Spoerri » 179

Wolff Heintschel von Heinegg » 183

Acronyms » 187

Acknowledgements

L'Istituto Internazionale di Diritto Umanitario ringrazia vivamente i Governi e gli Enti che hanno concesso un contributo finanziario o il patrocinio per la Tavola Rotonda.

The International Institute of Humanitarian Law warmly thanks the Governments and Organisations that have given either a financial contribution or their patronage on the occasion of this Round Table.

L'Institut International de Droit Humanitaire tient à remercier les Gouvernements et les Organisations qui ont donné leur appui financier ou bien leur patronage à l'occasion de cette Table Ronde.

BANDA DIPARTIMENTALE DELLA MARINA
BRITISH RED CROSS
CAMERA DI COMMERCIO DI IMPERIA
CASINÒ DI SANREMO
COMITÉ INTERNATIONAL DE LA CROIX-ROUGE
COMUNE DI SANREMO
CROCE ROSSA ITALIANA
CROIX-ROUGE MONÉGASQUE
DÉPARTEMENT FÉDÉRAL DES AFFAIRES ETRANGÈRES, SUISSE
ISTITUTO AFFARI INTERNAZIONALI
MINISTERO DEGLI AFFARI ESTERI, ITALIA
MINISTERO DELLA DIFESA, ITALIA
MINISTRY OF FOREIGN AFFAIRS, NORWAY
NORTH ATLANTIC TREATY ORGANIZATION
QATAR RED CRESCENT
REGIONE LIGURIA

Preface

Contemporary armed conflicts have increasingly seen the emergence not only of new actors but also of new armament technologies, which have resulted from the continuous technological development in the field of defence. From new robotic technologies to cyber-attack, passing through drones, energy weapons, satellite technology and space weapons – science fiction or not – radical changes have occurred in the definition of battlefields, fighting and combatants, and new challenges have arisen with respect to the applicability and the effective application of well established principles of International Humanitarian Law.

The XXXIV Round Table on current issues on International Humanitarian Law, organised by the Sanremo Institute in collaboration with the International Committee of the Red Cross, gathered distinguished academics, legal experts, military commanders and government officials for an in depth discussion of the legal and operational impact of technology on modern warfare, with a special emphasis on the legal questions and humanitarian concerns related to the use of robots and the new threats involved in cyber warfare.

In publishing the proceedings of the Round Table, the Institute wishes to warmly thank all those who contributed to ensuring the success of the event. I am confident that this publication will help to underscore the increasing importance of the promotion, teaching and enforcement of International Humanitarian Law in a rapidly changing security environment.

Fausto Pocar
President of the International Institute
of Humanitarian Law

I. Opening session

Opening remarks

Maurizio Moreno

Presidente Onorario, Istituto Internazionale di Diritto Umanitario, Sanremo

A nome dell'Istituto Internazionale di Diritto Umanitario mi sia consentito innanzitutto di rivolgere un cordiale benvenuto e un sincero ringraziamento a tutti i presenti, alle personalità, agli amici, ai soci che hanno voluto partecipare a questo grande incontro internazionale di settembre, organizzato – com'è tradizione – con la collaborazione del Comitato Internazionale della Croce Rossa di Ginevra. Vorrei rivolgere il più vivo grazie al Comune e al Casinò Municipale di Sanremo, per averci ancora una volta consentito di aprire i lavori in questa prestigiosa cornice.

La presenza stamani qui di un folto e qualificato pubblico proveniente da diversi continenti conferma come la Tavola Rotonda di Sanremo, giunta alla 34^a edizione, rappresenti a tutti gli effetti un appuntamento d'obbligo nell'agenda di quanti, a livello internazionale, hanno a cuore la promozione ed il rispetto del diritto internazionale umanitario: quel corpo di norme articolate e complesse che ha l'obiettivo di tutelare la dignità della persona umana e di mitigare le violenze e le sofferenze che scaturiscono dai conflitti armati.

Gli avvenimenti degli ultimi mesi, di questi giorni, in Libia e nel Mediterraneo – come già i diversi conflitti che sono andati susseguendosi a partire dalla fine della guerra fredda (dai Balcani all'Iraq, dall'Afghanistan all'Africa sub-sahariana) sono di fronte agli occhi di tutti, con il loro fardello di inutili atrocità e vittime innocenti. E ripropongono drammaticamente all'attenzione l'attualità e l'importanza di regole e principi umanitari di cui continuano a verificarsi inquietanti violazioni.

Il diritto umanitario è oggi certamente confrontato a nuove sfide, stenta a volte a trovare piena applicazione nei nuovi scenari operativi, perché le ragioni, la natura, gli strumenti e i protagonisti stessi della guerra sono cambiati.

Anche attraverso i media è facile rilevare come – nel campo dell'informatica, delle telecomunicazioni, dell'elettronica – sia da qualche

tempo in atto una vera e propria rivoluzione che ha profondamente trasformato le strategie militari e quelli che, nella guerra classica, si chiamavano i “mezzi e metodi di combattimento”. Sia nei più recenti conflitti sia nelle operazioni di mantenimento della pace condotte dalla Comunità Internazionale hanno trovato crescente impiego dispositivi telecomandati, satelliti, munizioni ad alta precisione, armi c.d. “intelligenti” il cui sviluppo dovrebbe idealmente consentire una più selettiva individuazione degli obiettivi militari e mettere al riparo le popolazioni civili da inutili perdite e devastazioni.

Anche in aree a noi non lontane, i civili continuano tuttavia ad essere le principali vittime di abusi e sopraffazioni, quando non si tratti di veri e propri crimini di guerra o contro l'umanità, che non possono lasciarci indifferenti.

I principi di umanità sono principi universali che affondano le loro radici lontano nei tempi: principi etici, prima ancora che giuridici, di rispetto della persona umana, di lealtà, di solidarietà internazionale, di garanzia della legalità e della giustizia anche quale veicolo per il ristabilimento della pace.

Della promozione e della diffusione di tali principi e norme, l'Istituto Internazionale di Diritto Umanitario ha fatto ormai da oltre quarant'anni la propria bandiera e la propria missione.

Il tema prescelto per questi lavori, d'intesa con il Comitato Internazionale della Croce Rossa, è di grandissima attualità ed è stato oggetto negli ultimi tempi di crescente attenzione sia da parte dei Governi, sia nell'ambito delle principali Organizzazioni Internazionali, suscitando un interesse che va ben oltre la cerchia degli addetti ai lavori.

As the pace of technological innovation continues to accelerate at breath-taking speed, a number of serious concerns and controversial questions have arisen about the legal and ethical aspects of the development and the use in modern conflicts of weapons and military devices – robots, unmanned combat vehicles, cyber technologies – which could lead to an erosion, if not a breakdown, of traditional consolidated standards of enforcement of international humanitarian law.

I do not think (and the ICRC has recently underscored this) that we are suffering from a legal vacuum. On the contrary! A legal regime exists, a coherent set of norms is there! And I am firmly convinced that nobody could seriously question the applicability of international humanitarian law to a warfare characterized by growing automation of military operations.

The rapid revolution of technology and the inexorable trend towards large scale employment on the battlefield of weapons that do not need

a soldier to pull the trigger open new prospects in military strategies and operations, and provide a tremendous opportunity to better protect civilians, to reduce cost and risk and to spare innocent lives in armed conflicts.

As technology evolves, the weapons the armed forces use must also, unavoidably, evolve. It has happened in the past. It will continue to happen in the future.

Everyone recognizes, however, that the pace and the scale of a process which is radically changing the security environment have brought to the attention new critical elements and tricky dilemmas. Ambiguities and uncertainties emerge in the reading of existing rules, sometimes challenging conventional wisdom. Scientists, lawyers, military commanders are engaged in discussions where opinions not always converge. The industry does not seem too keen to take an active part in the public debate, to share its knowledge and business interests.

A number of real questions are being raised today and not only by the humanitarian community, concerning the permissibility of specific new weapon technologies and the compatibility of their use with existing international norms.

Legal clarity is to a large extent a key element and a prerequisite of full compliance with existing norms. This meeting gives us the possibility to look closer into the matter.

Which are the principles and rules applicable to new technologies? How to comply with the norm introduced by the 1977 Geneva Additional Protocol I (article 35) that considers “not unlimited” the right of the parties to the conflict to choose methods or means of warfare? What about the concept of legal liability and personal accountability? Should a war crime be committed by a fully autonomous device? How to ensure the enforcement of the principles of proportionality and precaution in attack in scenarios where the attacker is thousands of miles away from the target? What are respectively the role and the responsibility of governments and industry with reference to the rule – article 36 of Additional Protocol I – according to which in the study, the development and adoption of a new weapon, means or method of warfare State parties are under the obligation to determine whether their employment would be prohibited by applicable international law?

These are only a few of the questions which could deserve serious consideration and I would like to express my deep gratitude to all those who are freely giving us today their time and expertise to improve our understanding of these issues and the related challenges.

What we should always keep in mind is that technology evolution is not an autonomous, independent process. It is a tool in our hands. Development

of technology and its applications are definitely dependent upon human decisions.

Mesdames, Messieurs,

Notre agenda est très chargé et je voudrais d'ici un moment donner la parole au Président du CICR, M. Jakob Kellenberger, pour son discours d'encadrement qui nous permettra de rentrer dans le vif du sujet.

D'après l'ordre du jour nos travaux se dérouleront selon les règles de Chatham House en toute liberté et dans un esprit d'ouverture et informalité propre à favoriser une ample participation de la salle. Après une discussion de caractère général sur les développements les plus récents des nouvelles technologies employées en milieu militaire, nous allons approfondir dans le détail deux grands thèmes spécifiques.

En premier lieu, la problématique ayant trait à la multiplication dans les zones de conflit des systèmes d'armements autonomes. C'est un thème passionnant, s'agissant d'armes qui sont de plus en plus utilisées, concurremment avec les armements traditionnels. Je lisais récemment dans une revue spécialisée qu'aux États-Unis les tâches d'un soldat sur cinquante sont désormais accomplies par des engins autonomes ou robotisés. Je crois qu'il est urgent de se soucier des enjeux éthiques et juridiques qui se profilent.

Le deuxième grand thème est celui de la guerre informatique, dont nous avons vu apparaître les premières manifestations: dissémination de virus, intrusions illégales, vols de données publiques et privées, attaques ciblés contre des réseaux stratégiques pour la sécurité.

C'est un défi complexe et actuel. Les actes d'agression informatique qui se sont développés à partir des attaques de 2007 contre l'Estonie ont obligé les États et les organisations internationales (à commencer par l'OTAN et l'UE) à revoir soigneusement leurs stratégies de défense et de protection des infrastructures qui peuvent devenir le cible privilégié d'une nouvelle forme de guerre ou d'actes de terrorisme utilisant le cyber espace.

Je crois que quelques remerciements s'imposent. Un merci à tous les participants venant de différents pays. Aux savants, aux juristes, aux militaires, aux diplomates qui ont accepté d'introduire les différents sujets. Un merci aux coordinateurs de cette Table Ronde: le Général de Brigade Erwin Dahinden, le Dr. Baldwin De Vidts, le Dr. Cordula Droege, le Prof. Wolff Heintschell von Heinegg et le Prof. Michel Veuthey, qui ont fait un travail remarquable. Et naturellement aux modérateurs qui vont assurer le bon déroulement des discussions: le Professeur Jacobsson, le Professeur Greppi, l'Ambassadeur d'Aboville, l'Ambassadeur Zellweger, Mme Droege.

Qu'il me soit par ailleurs permis d'exprimer la plus sincère gratitude aux Ministères Italiens des Affaires Étrangères et de la Défense qui ont

accordé leur patronage à cette initiative. Dans une conjoncture économique très difficile, l'organisation de cette rencontre n'aurait pas pu avoir lieu sans l'appui généreux d'un certain nombre de gouvernements et d'organisations qui méritent d'être spécifiquement mentionnés. A part l'Italie, la Suisse (dont je tiens à saluer chaleureusement le Secrétaire d'État aux Affaires Étrangères, M. Maurer qui interviendra au cours de cette séance), et puis l'OTAN, le CICR, et encore la Norvège; la Mairie de Sanremo; la Région Ligurie; l'*Istituto Affari Internazionali* de Rome; des Sociétés Nationales de la Croix-Rouge Britannique, Monégasque, et du Qatar (c'est à cette dernière que nous devons l'interprétation en langue arabe), la Chambre de Commerce d'Imperia.

Je ne saurais pas terminer ces propos sans vous faire part des sentiments d'émotion que j'éprouve au moment où je suis appelé à assumer, pour un deuxième mandat, la responsabilité de l'Institut de Sanremo.

L'Assemblée Générale a élu hier un nouveau Conseil dont la composition s'inscrit à maints égards dans une ligne de continuité. Je voudrais donner aux trois nouveaux élus ma plus chaleureuse bienvenue et dire en même temps à mes compagnons de route de la première heure qui ont été confirmés au sein du Conseil combien je suis heureux de pouvoir continuer à jouir de leur confiance et à travailler avec eux. A ceux qui nous quittent; un merci, un merci sincère et reconnaissant pour leur magnifique coopération.

Il me plaît aussi de souligner que par la suite de leur cooptation le nouveau Conseil continuera à bénéficier de la collaboration de personnalités éminentes telles que le Juge Owada, Président de la Cour Internationale de La Haye, et l'Ambassadeur Thompson, Directeur-Général Adjoint de l'OIM. Le CICR sera représenté au plus haut niveau par la Vice-Présidente Mme Beerli. Quant' aux membres institutionnels, M. Guerra continuera à représenter la Croix-Rouge Italienne; la Mairie de Sanremo vient de désigner Maître Berrino comme son représentant au sein du Conseil. Le nouveau Conseil a confirmé Mme Baldini comme Secrétaire général et M. Giancaterino comme Trésorier.

J'ai accepté ce deuxième (et d'après les statuts dernier) mandat non sans quelques hésitations car je crois que l'Institut a intérêt à s'ouvrir davantage vers les générations plus jeunes. Je l'ai fait avec tous les autres membres du Conseil dans un esprit de service et de responsabilité, répondant à un appel précis de nombreux membres et amis de l'Institut, de gouvernements et d'organisations internationales qui, en soutenant généreusement nos activités, ont apprécié ce que nous avons réalisé ces dernières années et nous ont demandé de porter à terme la restructuration de l'Institut selon les lignes du plan stratégique récemment adopté. Dans une situation

économique préoccupante nous avons devant nous des échéances qu'il faut affronter en serrant les rangs, en redoublant nos efforts, dans un climat de confiance et de coopération grandissante entre le Conseil qui vient d'être élu et l'ensemble des membres de l'Institut.

Cette Table Ronde sera pour le nouveau Conseil aussi l'occasion pour être à l'écoute des nombreux amis de l'Institut qui sont aujourd'hui dans cette salle, pour recevoir leur avis, pour retenir des idées qui puissent contribuer à notre action.

Welcome address

Giovanni Berrino

Assessore, Comune di Sanremo

È per me motivo di grande soddisfazione porgere, a nome dell'Amministrazione Comunale, il più caloroso benvenuto alle illustri Autorità e ai graditi Ospiti che partecipano a questo importante Convegno internazionale.

Sono ormai più di trent'anni che la Città di Sanremo ha l'onore di ospitare in settembre questa Tavola Rotonda dedicata all'approfondimento delle tematiche umanitarie di più pressante attualità.

Promosso congiuntamente dall'Istituto Internazionale di Diritto Umanitario di Sanremo e dal Comitato Internazionale della Croce Rossa di Ginevra con il pieno appoggio del Comune, è questo un incontro di grande rilievo, che ben corrisponde alla vocazione e alla tradizione di Sanremo, fin dalle sue origini crocevia di scambi e d'incontri tra le nazioni. Se ancora una volta un gruppo così folto ed autorevole di rappresentanti di governi, insigni studiosi, alti ufficiali delle forze armate provenienti dai diversi continenti, è convenuto in questa Città lo si deve certamente all'urgenza e all'importanza dei temi in discussione, ma ritengo anche – mi sia consentito dirlo abbandonando ogni falsa modestia – alle rodiate capacità di accoglienza e allo straordinario contesto ambientale che Sanremo offre per l'organizzazione di convegni internazionali di questo tipo.

Nei giorni a venire sarete chiamati a discutere di problemi che vivamente preoccupano non soltanto i Governi e le Organizzazioni Internazionali direttamente interessate, ma, sempre più, nella loro più ampia accezione, la società civile e l'opinione pubblica. Tutti noi siamo quotidianamente esposti alle immagini di sofferenza e di morte che ci vengono dai numerosi focolai di crisi e di confronto armato attivi in tutto il mondo: fino alle porte di casa nostra, la sponda sud del Mediterraneo, dove si consumano preoccupanti atrocità contro la popolazione civile.

L'Istituto Internazionale di Diritto Umanitario svolge un importante ruolo oltre che come centro di alta specializzazione e formazione, come

foro di riflessione sulle questioni più importanti con cui l'umanità si confronta. Le discipline di cui l'Istituto si occupa – il diritto internazionale umanitario, il diritto dei migranti, il diritto dei rifugiati – sono in una società ormai globalizzata, discipline intimamente correlate, che suscitano un crescente interesse non soltanto presso gli addetti ai lavori. Anche in quest'ottica, l'Amministrazione Comunale di Sanremo è impegnata a sostenere le attività dell'Istituto, nella piena consapevolezza dei loro importanti ritorni sul territorio.

Anche a nome della popolazione di Sanremo, vorrei porgere a tutti i presenti il mio augurio di buon lavoro, nella fiducia che possiate trovare durante il vostro soggiorno anche il tempo per scoprire le bellezze e le attrattive di questa città. Sanremo sarà lieta di tornare ad accogliervi in futuro, con il suo clima, il suo mare, i suoi fiori, con il senso di ospitalità che la contraddistingue.

Keynote address

Jakob Kellenberger

President, International Committee of the Red Cross, Geneva

New technologies and new weapons have revolutionized warfare since time immemorial. We only need to 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 grams, 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.

At the same time, while banning a very specific weapon, the St. Petersburg Declaration already set out some general principles which would later reform 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 recognized 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 cyberspace 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 rely.

Another difficulty in applying the rules of international humanitarian law (IHL) to cyberspace, stems from the digitalization on which cyberspace is built. Digitalization 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, which we will be discussing at this Round Table, is 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 minimize 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.

I thank the International Institute of Humanitarian Law for hosting this Round Table and I thank all of you for your interest in engaging with us in reflection and debate. I wish you fruitful and successful discussions.

Statement

Peter Maurer

Secretary of State, Federal Department of Foreign Affairs, Bern

First, I wish to express my sincere appreciation to the Sanremo Institute and the ICRC for their important work in the promotion and dissemination of International Humanitarian Law (IHL). Switzerland has been cooperating with the Institute for many years, in particular through the yearly Round Tables. We value the Organizers for their “convening power” and the Round Tables for representing a major event in the world of humanitarian law. They offer an important opportunity for informal dialogue and constructive debate between members of scientific, diplomatic and military circles from all over the world. This is again particularly important in view of the 31st International Conference of the Red Cross and Red Crescent in November.

The topic of this year’s Round Table is timely. Technological developments have a significant impact on both the means and methods of warfare. Information technology has transformed the planning of military operations. It has also changed the targeting as well as the capacity of the military to conduct operations in complex and remote environments. Network technology has redefined the boundaries of the battle space, which includes multiple actors in military decisions through an expanding chain of command across continents, countries and agencies. These developments have increased the need to clarify international humanitarian law, and to better understand how these technologies are used to ensure and enhance protection of civilians and civilian objects in situations of armed conflict.

Paradoxically, technological developments have offered interesting opportunities to improve the protection of civilians, by facilitating the gathering and analysis of information on the conduct of hostilities or the monitoring of vulnerabilities in complex emergencies. Never before has the international community been better informed on threats against

populations in situations of armed conflicts – at least in certain conflicts. Thanks to information and networking technology, political and professional actors around the world have an enhanced capacity to provide timely assistance, and to take necessary steps to ensure compliance with the rules of IHL. Whether they can transform such capacity into real action remains debatable and dependent on many other factors as well as new technologies.

In short, and not surprisingly, technology does not have, as such, positive or negative impacts on the realization of core humanitarian objectives; it offers though another dimension to humanitarian work.

Switzerland – as a State Party and Depositary of the Geneva Conventions and their Additional Protocols – has over decades engaged to maintain the relevance of IHL. We strongly support the conclusions of the ICRC’s study on “Strengthening Legal Protection of Victims of Armed Conflicts”, which highlights the importance of better compliance with existing law and defines areas for its strengthening. We are convinced that such efforts need a more structured and systematic engagement from High Contracting Parties. This is also one of the reasons why we have appointed an Ambassador-at-large for the application of IHL. Today’s debate on the use of modern technology and IHL are thus part of a larger agenda to strengthen the law.

Recently, Switzerland has invested in the exploration, study and development of emerging technologies and their impact on the protection of populations in contemporary armed conflicts. While we are convinced that, also in this context, IHL remains an adequate framework, we do hope that some unresolved questions can be debated here in Sanremo and find their way into the ICRC’s Challenges Report for the 31st International Conference in November. Such questions include efforts to understand more clearly how new technologies, like automated weapons systems, drones and other weaponry, can be aligned with fundamental humanitarian principles such as distinction, proportionality and military necessity.

In this context, I would like to highlight recent efforts to build upon the core IHL rules and to enhance protection while responding to technology challenges. In particular, I would like to mention the “International Humanitarian Law Initiative’s Manual on Air and Missile Warfare”, adopted in Bern in May 2009 by a group of international experts, many of whom I am glad to see present here today¹. This initiative was

1. From the speaker list, members of the Air and Missile Warfare (AMW) expert group present in Sanremo include: Marie Jacobsson (Sweden), Prof. Wolff Heintschel von Heinegg (Germany), Prof. Marco Sassóli (Switzerland), Air Commodore Bill Boothby (United Kingdom), Prof. Michael Bothe (Germany and President of the Fact Finding Commission) and Prof. Yoram Dinstein (Israel).

launched with the purpose of providing an authoritative interpretation of international law applicable to a specific high-tech domain. It has impacted upon the planning of air operations and training of air officers on several continents, thanks to the continued engagement and support of some of the members of the group of experts under the auspices of the Geneva Centre for Security Policy.

As mentioned before, information technologies are offering the possibility to gather and analyse data in real time. Satellite systems are collecting information on population movements, mapping refugee camps, surveying battlefields for potential violations of IHL and providing assistance to protection agencies in times of humanitarian crises. Network technology is supporting an expanding web of professionals and agencies, sharing information on their observations and activities in the most remote and hazardous environments, thereby upgrading the capacity of humanitarian agencies to offer assistance and protection in a timely and effective manner. Multiple IT platforms, some supported by my country, like ReliefWeb, ICT4Peace, the IHL Research Initiative and Forum, are providing vital real-time information to hundreds of thousands of professional users worldwide on current vulnerabilities of populations, applicable laws, policy interpretations and operational recommendations. More recently, Switzerland supported the development of a monthly Live Web Seminar series on the implementation of IHL, gathering over 3,000 professionals worldwide from governments, humanitarian agencies and the military. My country has also expanded its longstanding commitment to teaching and discussion on IHL including support for a comprehensive set of online courses on IHL for professionals. While such use of technology is potentially transforming humanitarian action, it is also obvious that enhanced knowledge does not necessarily translate into improvements, unless it is informing action by engaged individuals and organizations on the ground and close to the victims.

In recent years, cyberspace has become an emerging issue in need of regulation. One should recall that clarification attempts around cyber operations began to draw the attention of the International Community in the late 1990s. The United States Naval War College convened the first major conference on the subject of computer network attacks and international law in 1999, and the first international treaty on cyber-crime was adopted in Budapest in 2001. During the 28th International Conference of the Red Cross and Red Crescent in 2003, Sweden, Switzerland and Finland made a pledge with regard to computer network attacks during armed conflict. Subsequently, at the end of 2004, Sweden hosted an international expert conference on the issue. Although these first steps

towards clarifying the interpretation and application of international law in cyberspace had generated a certain momentum, the events of 11 September 2001 and the ensuing military and counter-terrorist campaigns in Afghanistan, Iraq and elsewhere increasingly diverted attention from the topic. It was not until 2007, when Estonia became the target of massive cyber attacks, that the spectre of cyber warfare suddenly regained centre stage. The subsequent use of cyber operations in other conflict situations renewed awareness of the vulnerability to services and infrastructures, and the lack of agreed standards of acceptable behaviour in cyberspace.

We take good note of current efforts to develop a “Manual on International Law Applicable to Cyber Conflict” which is currently being elaborated by NATO’s Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia. We hope that the Tallinn Manual will be consulted broadly in order to determine whether or not this work could serve as a starting point in gathering State consensus on international norms governing State conduct in cyber operations.

In concluding, I trust that this year’s Round Table will allow us to take a closer look at the legal and operational impacts of new weapons and military technologies. I thank the organizers in particular for having accepted Switzerland to chair a panel discussion tomorrow. I am looking forward to fruitful discussions. Let us keep in mind that IHL’s key objective is to maintain a minimum standard of humanity in armed conflict. It is, therefore, our responsibility to keep this body of law fit to fulfil its fundamental mission. IHL must be able to respond to the challenges posed by technology, but it also has to be mindful of the great opportunities of new technologies in enhancing protection efforts.

Statement

Vincenzo Camporini

Former Chief of the General Defence Staff – Special Advisor for Military Affairs of the Minister of Foreign Affairs, Rome

When a soldier retires, he thinks he will have time to relax, to take care of his family and to pursue his hobbies. Unfortunately for me, this has not been the case. However, I am very grateful to my good friend, Maurizio Moreno, who called me back for this Round Table, which is, in my opinion, of great importance for the development of International Humanitarian Law.

Every soldier who was operational during the Cold War will recall the good old times when things were clear and when war was a concept intrinsically symmetric. Armed conflict consisted in the confrontation of an army against another one and the fighting was done following extremely precise rules that would lead to a clear victory of one army over the other.

The fall of the Berlin Wall marked the beginning of a new area, which proved to be much more troubled than expected. Not only the rules in fighting changed dramatically, but also the concept of symmetry itself was challenged, as the 9/11 attacks illustrated. Following this attack, the concept of asymmetry began to spread out in vocabulary of practitioners and policy-makers.

The first level of asymmetry refers to the means used by combatants. A normal army uses guns and bombs, and now the opponent uses other means, which were not originally intended to be employed in an armed conflict. In my opinion, this would be a very short sighted definition of the concept of asymmetry. Indeed, this concept does not only refer to means, but it also and mostly refers to mind-set. Asymmetry refers to the different perceptions actors involved in armed conflict have on the use of force. On the one hand, there are those who agree that the use of force may be necessary but must be limited by precise rules, aiming at preserving the roots of humanity. On the other hand, there are those who believe they can use any means and type of violence against anybody because their enemy is not a combatant, but the 'Other'. This is, in my opinion, the real asymmetry.

In operational terms, asymmetry refers to the distinction between those who aim at eliminating the threat with the use of force and those who still aim at breaking the opponent's will by any means available. Not too long ago, the latter was also our mind-set as the indiscriminate bombings during the Second World War exemplify. The principles encompassed in the 1920s' and the 1930s' Air Force doctrines, guiding the use of air power, also show that our previous position was to break our enemy's will, at any cost.

Nevertheless, in the last decades, we have made significant progress and we have to be proud of it. We have to be proud of this asymmetry in contemporary conflicts. We must resist the temptation to go back to old patterns and to adopt the same behaviour of those we designate as our enemies.

This is why I laud this Round Table and I think the message we should promote during the next three days is that asymmetry is the evidence of the progress of mankind.

Statement

Betty E. King

Permanent Representative of the United States of America
to the United Nations Office and other International Organizations, Geneva

I am delighted again to be a part of this annual roundtable. The United States has been a supporter of the International Institute of Humanitarian Law (IIHL) and a participant in its events for over a decade.

We continue to value the Institute's work and are especially proud to support the Institute's refugee law courses to promote and disseminate knowledge of refugee protection. These courses directly support a shared strategic objective to develop and reinforce protection capacity in priority host countries. We are pleased that the refugee law courses focus on the application of human rights and the protection of refugees, emphasizing protection as the nexus between human rights and refugee law.

Last year, the Institute began a period of transition which continues today. We laud the Institute's efforts to develop more participatory courses to demonstrate better the impact of its training and to broaden significantly its donor base. We welcome the fact that the Institute has reached out increasingly to non-governmental partners, including foundations and universities, and we are especially encouraged that the Institute has set targets for increasing its funding from non-governmental sources by the end of 2012.

Looking back at the Institute's record, we see thousands of government and military officials, international organization and civil society representatives who have come to Sanremo to learn about International Humanitarian Law and Refugee Law. They have exchanged ideas on the application of these principles and the future of humanitarian affairs. And most importantly, they have gone on to practice what they learned, to build on their experience here, to improve their humanitarian practices at home, and to better the lives of vulnerable people around the world. This is no small achievement for which we are all grateful to IIHL.

I believe the subject of this year's roundtable is especially topical. The world in which we are living is rapidly evolving, and – almost daily – new

technologies challenge past assumptions. As a representative of President Obama, I am proud to be with you here to demonstrate the United States' commitment to ensuring global compliance with the laws of war. I think it is worth repeating President Obama's remarks when he accepted the Nobel Peace Prize regarding the changing nature of war and its combatants. He said, "There will be times when nations – acting individually or in concert – will find the use of force not only necessary but morally justified". But he also recognized that while "... the instruments of war do have a role to play in preserving the peace... this truth must coexist with another – that no matter how justified, war promises human tragedy".

We won't see an end to that human tragedy in our lifetime, or perhaps ever, but this reality only enhances our imperative to reduce the human cost of war, even as the means of warfare evolve. The law of war must be applied appropriately to evolving realities and governments have the duty to ensure that the rules governing their actions in war remain vital.

As President Obama also affirmed in his Nobel lecture in Oslo, "[...] adhering to standards, international standards, strengthens those who do, and isolates those who don't". Both President Obama and Secretary of State, Hillary Clinton – two outstanding lawyers – have reiterated our commitment to living our values by respecting the rule of law, understanding, as they do, that by imposing constraints on government action, law legitimizes and gives credibility to governmental action. In this context, the United States agrees fully that international humanitarian law remains the appropriate framework for regulating the conduct of parties to both international and non-international armed conflicts. And we believe that the principal focus of our efforts should be on promoting greater compliance with existing legal frameworks.

Allow me now just to say a few words related to the topic of this year's roundtable. Some have challenged *the very use* of advanced weapons systems. But there is no prohibition under the laws of war on the use of technologically advanced weapons systems in armed conflict – such as pilotless aircraft or so-called smart bombs – so long as they are employed in conformity with applicable laws of war. Indeed, using such advanced technologies can ensure both that the best intelligence is available for planning operations and that civilian casualties are minimized in carrying out such operations.

Statement

Carmin De Pascale

Head of the Department Armaments Policy, Ministry of Defence, Rome

The topic of this first day of debates, “humanity and technology: convergence and antagonism”, addresses an issue that is obviously still open, that is, the converging or conflicting aspects of humanity and technology. We shall intend humanity in its most general sense, that is, both as humankind and as the respect of human rights and of the planet we inhabit and its environment.

The foundation of humanitarian international law lies on the necessity of ensuring that the people’s fundamental rights, that are by now a recognized asset of the international community’s juridical culture, are respected even in such an extreme situation as an armed conflict.

The complex system of rules and customs, which constitutes international humanitarian law, hinges on a few fundamental principles. Their “golden rule” is summarized by art. 35 of the 1977 Additional Protocol I to the Geneva Conventions: the right of the Parties to the conflict to choose methods or means of warfare is not unlimited.

Although sometimes with a regrettable delay, the technological development and augmented power and destructivity of weapons have been luckily followed by the increasing awareness of peoples and governments of the importance of respecting humanitarian principles.

In fact, after the declarations of St Petersburg (1868) and The Hague (1899)¹, a further adjustment of the international regulation on conventional weapons did not occur until 1980 with the “certain conventional weapons”, followed over the years by 5 protocols². Such process was concluded in the

1. Renouncing the use of explosive or incendiary projectiles under the weight of 400g and prohibiting dumdum bullets respectively.

2. The 5 protocols concern: fragments non detectable by X-rays (1980); landmines, traps and other explosive devices (1980); incendiary weapons (1980); blinding laser weapons (1995); explosive remnants of war (2003).

nineties and 2008 with the signature of the Convention on Anti-Personnel Mines (1997 Ottawa Convention) and on cluster munitions (2008 Dublin-Oslo Convention). Regarding the latter, I would like to point out that Italy will shortly sign a memorandum of understanding with France and Germany for the upgrade of the MLRS system (multiple launch rocket system), having regard for the obligations laid down by the mentioned Convention, that is, equipping it with the GMLRS unitary rockets with monolithic warhead.

It is obvious that the technological development of weaponry and the production of new and more advanced arms have often been in contrast, or, to reflect the title of today's topic, antagonistic to the principles of humanity that we have discussed so far. International humanitarian law often did nothing but "try to catch up", in an effort to prevent or restrict the use of certain new weapons in order to eliminate or at least reduce their devastating and indiscriminate effects.

In recent years, however, maybe under the influence of the new international scenarios and of the cogent limitations to the use of force in such operational contexts, military technology has, in my opinion, made a lot of progress in the direction of a greater respect of the fundamental international humanitarian law principles previously mentioned. In this respect, the Secretariat General of Defence and National Armaments Directorate plays a key role on the basis of the relevant legal provisions, which identify in the leader of said structure "... the person responsible for the activities of research and development, production and procurement of weapon systems".

Technological research is not mentioned by chance: it is strategically essential for any complex organization and, as you can imagine, for the defence sector in particular.

The Secretary-General/NAD must promote and coordinate military research and technology, harmonizing global defence requirements and integrating them with the initiatives promoted by other players, nationally (for example, by industry, university and research centres), as well as internationally within NATO (NATO RTO) and the EU (LOI-ETAP/European Technology Acquisition Programme), and OCCAR (to mention just the most important ones). Their achievements are thus transformed into actual technological innovations, which can be applied to new means and equipment that allow the Italian armed forces to intervene with the utmost security and with due regard for the fundamental principles of international humanitarian law³.

3. Art. 36 of the 1977 Additional Protocol I lays down 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 be prohibited by the rules of international law.

For example, the attacking party's adoption of precautionary measures (principle of precaution – as provided for by art. 57 of the 1977 Additional Protocol I), such as the possibility of directly verifying the target during the conduct of military operations or of keeping a communication channel open at all times with those responsible for preparing or deciding the intervention so as to modify their conduct when new information is acquired, has been made possible by the technologies currently at our disposal.

The use of UAV aircraft has allowed for the notable reduction in the risk of casualties, while permitting a realistic assessment of targets and limiting the chance of identification mistakes. In fact, such systems allow for the instantaneous sharing of information on the position of emplacements and the movements of enemy troops, including GPS satellite data, and thus allows the choice of the most appropriate carrier to intervene in the situation in question with regard to both the principle of distinction (according to which in a conflict only military targets can be attacked) and the principle of proportionality.

For what concerns future developments in this field, Italy participates, for example, in the LOI-ETAP with other European nations. The purpose of this programme is to identify the technologies (such as radar, navigation and communication systems) that can be used on future manned and unmanned aircraft.

But while on the one hand technology proves helpful, on the other hand it poses new challenges, such as cyber attacks aimed at destroying IT networks and databases. This is the so-called cyber warfare, to which one of the five sessions of this round table will be devoted.

All of you probably remember the 2007 cyber attack against Estonian institutional websites, following which the NATO nations decided to increase their cyber defence capabilities, and eventually established the Cyber Defence Management Authority (CDMA) in 2008.

The new NATO cyber defence policy, recently approved by the allied Ministers of Defence, introduces significant innovations compared to the previous 2008 document. Incorporating the cybernetic aspects of modern conflicts in the strategic doctrine, it fits well in the new general scenario. The starting point of the new policy is, in fact, the definitive assimilation of cyberspace to the four other traditional domains (sea, air, land and space) and the understanding that cyberspace security is one of the greatest challenges the Alliance has to face.

Undeniably, cyber warfare is very close to traditional war for what concerns its impact: this is due to the fact that technological evolution has allowed to join all forms of command, control and data management on IT platforms. Consider, for example, the possibly devastating consequences of

a sabotage of airspace control systems. Under every respect, the use of this instrument could cause damages as serious as, or even more serious than, a conventional terrorist or military attack, including the direct loss of human lives. It is, therefore, completely obvious that cyber warfare should be restrained by the general principles of international humanitarian law too.

Unfortunately, nowadays it is still very difficult, if not impossible, to impute with certainty a cyber attack to its perpetrators. In any case, that would require very long analysis, which would necessitate the cooperation of the nations from which the attack originated or through which it transited. So, at present, it is evident that the threat of a military response or the enforcement of sanctions is still regarded by attackers as something unlikely and, therefore, with little deterring power.

So, what can I say in conclusion?

The history of weapons is characterized by the fight between bullet and armour, between cannon and fortress. The invention of new means of attack leads to the introduction of new means of defence, followed in its turn by the development of possibly even more destructive means. This process has been in place since the dawn of time and will most likely go on and on.

New international scenarios show that an overwhelming majority of the violations of international humanitarian law and human rights occur in so-called asymmetrical conflicts, where subversive movements, terrorist groups, are engaged, even though they aren't always equipped with technologically advanced weapons. In the current scenarios the purpose of military operations is more and more often to facilitate a peace and stabilization process in an area of crisis. In these situations it is of vital importance to prevent collateral damage, in order to facilitate the fulfilment of the mandate and not to risk harming the international community's credibility. We need to research, design and develop systems to adequately meet the requirements of our operational commitments, while respecting the principles of international humanitarian law. This challenge can be met only with an increasingly quicker and more effective response capability, and for this reason the secretariat has recently kicked off the operational phase of a deep structural reorganization.

In conclusion, I would like to state a basic and, I believe, inalienable principle: in our time, and even more in the years to come, it is necessary to recognize the superiority of human rights needs. Only this can ensure the respect of the international humanitarian law principles, which should inspire any man and woman irrespective of their political ideas, culture of origin, religious faith or, if you like, the technological progress achieved by them.

And with this I have concluded.

Statement

Laura Mirachian

Permanent Representative of Italy to the United Nations Office
and other International Organizations, Geneva

I am very pleased to be here, for the first time, among real friends: Ambassador Moreno, President of the International Institute of Humanitarian Law, and Dr. Kellenberger, President of the International Committee of the Red Cross (ICRC).

First, I take the opportunity to convey, once again, my deep appreciation for the ICRC's work, which is of great importance. For instance, in Syria, where a very difficult situation is persisting, the ICRC was among the very few organizations able to enter the country.

Now coming to the point, I am pleased to be here because this Institute has always been very successful in anticipating major humanitarian debates. Last year, which marked the 40th anniversary of the Institute, the Round Table was dedicated to the issue of global violence, with a special focus on terrorism, urban violence, piracy and forced disappearances.

This year the theme is the challenge represented by the increasing use, in contemporary armed conflicts, of new weapon technologies, satellite technologies, cyber warfare and, as General Camporini observed, by asymmetric conflicts which jeopardize the International Humanitarian Law traditional framework.

The outcome of this Round Table will, I am sure, contribute to enriching the agenda of the 31st International Conference of the Red Cross and Red Crescent and to promoting debates around further possible development of International Humanitarian Law. Development of this body of international law represents the heart of the ICRC's work, and it will possibly be discussed at the Conference next November. Due to the high level of expertise of the participants, this Round Table's outcome will certainly contribute positively to the success of the ICRC Conference.

Italy, as a country strongly engaged in disarmament issues and in the protection of civilians in armed conflicts, cannot underestimate the need

for an advanced legal framework covering new warfare technologies, including cyber warfare and non-lethal weapons in general. Hence, I wish to express my deep appreciation for the role of this Institute, which is widely recognized as a centre of excellence both in Italy and among the international community for its training courses in the fields of International Humanitarian Law, Refugee and Migration Law. Its historical cooperation with ICRC, IOM, UNHCR and the support provided by many States bear witness to the Institute's outstanding reputation. We are really proud to host it in Italy and we are proud of Ambassador Moreno directing this Institute and its work.

The Sanremo Institute has been organizing seminars and workshops all over the world, beyond the borders of Europe, in order to promote the discussion on central themes to International Humanitarian Law's development and the innovative and multi-disciplinary approach, used in all its activities, has enhanced the Institution's credibility beyond the limited boundaries of Italy and Europe.

I conclude by saying that we are proud to be able to continue supporting the International Institute of Humanitarian Law in very difficult financial circumstances and we will very much try to do so in the forthcoming years. I wish you all, fruitful work and a pleasant stay in this beautiful city.

Statement

Francesco Rocca

Extraordinary Commissioner of the Italian Red Cross, Rome

Sono molto lieto di partecipare all'apertura della xxxiv Tavola Rotonda dell'Istituto Internazionale di Diritto Umanitario di Sanremo e desidero salutare le numerose autorità politiche, militari e gli autorevoli esponenti del Movimento Internazionale della Croce Rossa presenti oggi.

Quest'anno il tema prescelto evidenzia ancora una volta la capacità dell'Istituto, a cui la Croce Rossa Italiana da sempre offre un pieno sostegno, di porre all'attenzione del mondo accademico, diplomatico e militare le questioni più sensibili nell'attuale agenda del diritto internazionale umanitario, rispetto alle quali si rende necessaria una riflessione. Le "nuove tecnologie" ed il loro impatto sulla disciplina non sono più un mero scenario futuribile, di interesse per soli pochi Stati tecnologicamente sviluppati, ma ormai, in diverse delle ultime campagne belliche o in situazioni post-conflittuali caratterizzate da rilevante tensione nelle aree delle operazioni, siamo giunti alle prime concrete applicazioni sul campo, che già hanno manifestato l'evidenziarsi di alcune concrete problematiche giuridiche ed umanitarie.

Basti pensare in proposito, quanto ad ipotesi che solo fino a pochi anni fa sembravano confinate ad una mera curiosità intellettuale, ai casi di "cyber warfare" attestati nel corso del conflitto armato internazionale intervenuto nel 2008 fra Russia e Georgia. La novità prospettata dallo scenario di cyber warfare è stata ben evidenziata dalla Commissione internazionale di accertamento dei fatti istituita dall'Unione Europea che, però, si è poi trovata in evidente difficoltà nell'operare una valutazione giuridica sulla vicenda. Concreto rilievo hanno ormai i sistemi di arma e di identificazione a controllo remoto che, in appena un decennio, a partire dal conflitto in Afghanistan del 2001, sono divenuti un elemento imprescindibile nelle operazioni belliche degli Stati tecnologicamente più avanzati. Ugualmente nota è la problematica sorta con le cosiddette "armi

non letali”. Lo stesso termine comunemente impiegato è però largamente fuorviante, dato che numerosi sono gli esempi, specie in operazioni condotte nell’ambito di contesti di law-enforcement, di effetti di carattere letale derivanti dalla natura stessa di alcuni di questi sistemi d’arma o da casi di improprio utilizzo dei medesimi. Inoltre, data l’eterogeneità dei sistemi di arma che sono comunemente ricompresi in tale ambito, questi si prestano ad una difficile complessiva valutazione con, in molti casi, l’esigenza di procedere ad un più approfondito e ponderato scrutinio sugli effetti ultimi causati a danno delle persone coinvolte e dell’ambiente, dato che, spesso, siamo in presenza di dati empirici modesti e contraddittori, che rendono ancora prematura ogni valutazione circa la loro legittimità.

Di conseguenza è fondamentale comprendere se le nuove tecnologie possano essere un ausilio rispetto ad una più puntuale applicazione dei basilari principi umanitari oppure se queste rischiano di rappresentare un ulteriore elemento di frizione all’interno del sistema. Quale Croce Rossa Italiana non possiamo ovviamente offrire analisi tecniche sul tema e specifiche osservazioni sulle novità presentate da taluni sistemi di arma o metodi di combattimento, ma dobbiamo nondimeno ribadire il quadro entro il quale gli sviluppi tecnologici promossi dagli Stati devono necessariamente porsi.

In molti casi è evidente che gli sviluppi tecnologici abbiano positivamente contribuito a ridurre le calamità causate dai conflitti. Basti pensare alla maggiore accuratezza evidenziata negli ultimi anni per alcuni sistemi di arma, come nel caso dell’armamento di precisione utilizzato negli attacchi aerei, che ha trovato un impiego sempre maggiore da parte degli Stati. Per evidenziare il trend verso cui si sta orientando la prassi contemporanea, si può ricordare come quello che mediaticamente veniva rappresentato come il primo caso di “guerra chirurgica”, ovvero il conflitto del Golfo del 1990-1991, vide un impiego estremamente modesto dell’armamento aereo di precisione, pari a solo il 7-8% del munizionamento impiegato dagli aeromobili occidentali, mentre in più recenti campagne aeree questo valore si attesta ormai oltre il 70%. Sempre più, conseguentemente, come ribadito recentemente anche nel Manuale di Harvard sulla guerra aerea e missilistica, si va correttamente affermando la tendenza a considerare unicamente questo tipo di armamento adatto ad essere impiegato in ambiente urbanizzato, dato che questo è il solo a facilitare l’applicazione di basilari principi del diritto umanitario. Questo positivo esempio non è ovviamente isolato, dato che ad esso possono affiancarsi le maggiori capacità di identificazione, e quindi, potenzialmente, di maggior rispetto degli obblighi di distinzione e precauzione negli attacchi, offerte, ad esempio, dai velivoli a controllo remoto senza pilota,

che, però, dinanzi ai prospettati sviluppi in materia, quali gli armamenti automatici che verranno discussi nel corso della Tavola Rotonda, appaiono ormai quasi come delle applicazioni tecnologiche già superate dal corso degli eventi.

Se queste esemplificazioni possono evidenziare un positivo riflesso delle innovative applicazioni tecnologiche negli scenari conflittuali, nondimeno, non deve essere sotteso come anche gli eventuali miglioramenti tecnologici offerti non possono affatto esentare le parti al conflitto dall'adempimento dei loro obblighi giuridici in materia e da un attento scrutinio circa le decisioni finali sul terreno. In fin troppi casi, in recenti conflitti, si sono dovuti registrare episodi di dubbia legalità, in cui anche gli ausili tecnologici impiegati dagli Stati negli attacchi in oggetto non hanno escluso che questi ultimi conducessero azioni che difficilmente apparivano compatibili con basilari principi del diritto umanitario. Lo sviluppo tecnologico non è quindi, aprioristicamente, sintomatico di una perfetta o migliore applicazione della normativa, a cui può condurre solo una puntuale attenzione verso l'applicazione, nelle concrete vicende, di corrette valutazioni giuridiche. Ugualmente, questi nuovi scenari, ripresentano ed accentuano il problema di quale sia lo standard tecnologico e quindi, di riflesso, quello normativo, che deve ritenersi applicabile nel conflitto armato, dato che, in presenza di Parti al conflitto caratterizzate da un'asimmetria tecnologica, occorre parimenti interrogarsi sul riflesso di questa situazione rispetto allo scrutinio che deve effettuarsi sulla condotta bellica.

Come sicuramente verrà evidenziato in questa Tavola Rotonda molti interrogativi si pongono rispetto a talune innovazioni tecnologiche che appaiono in grado di impattare negativamente sulla condotta dei conflitti armati e, in alcuni casi, è necessaria una riflessione ulteriore per comprendere quanto e come, basilari principi del diritto umanitario, come quello di distinzione, potranno essere messi in discussione in questi ambiti.

Si pensi, a mero titolo di esempio, ad eventuali futuri casi di cyber warfare e ai potenziali effetti sulla popolazione civile. Se nel 1991, dopo il conflitto nel Golfo, il futuro premio Nobel Martii Athisaari, inviato nell'area dal Segretario generale delle Nazioni Unite, poteva stigmatizzare come, a seguito degli attacchi alla rete elettrica, l'Iraq era stato relegato ad una fase pre-industriale, ma con tutti gli inconvenienti derivanti dalla dipendenza, tipici di una società post-industriale, dall'uso estensivo dell'energia e della tecnologia, non dissimili potranno essere le negative conseguenze in casi di estesi attacchi informatici che compromettano l'intero sistema della Rete. In questa ipotesi i rischi che attacchi al sistema Web possano compromettere il principio di distinzione sono evidenti ed ancora incerte sono le valutazioni sui potenziali effetti causati in moderne

società tecnologiche, che si affidano ad esso per lo svolgimento di sempre più capillari e fondamentali servizi di interesse per la popolazione. Ugualmente non va sottovalutato come ormai anche molte attività di carattere umanitario, basilari per lo stesso Movimento di Croce Rossa, siano strettamente dipendenti dal Web. Oltre alla comunicazione volta a facilitare le indispensabili attività umanitarie nei più difficili scenari operativi, basti pensare, a mero titolo di esempio, come anche lo stesso compito di facilitare il ristabilimento dei legami familiari in occasione di conflitti armati o disastri naturali siano ormai largamente dipendenti da un efficace funzionamento del sistema informatico e non più, ovviamente, affidate ai pregressi “messaggi di Croce Rossa”.

Ugualmente, il principio di distinzione rischia di risultare compromesso in ragione del sempre maggiore coinvolgimento, attestato in numerosi conflitti, di personale civile nel mantenimento e funzionamento di sistemi di arma tecnologicamente sviluppati. Proprio la natura altamente specializzata di alcune tecnologie attualmente impiegate ha reso evidente, specie nelle prime fasi di utilizzo, la rilevante dipendenza di alcune forze armate dal personale civile proveniente dall'industria del comparto bellico che fornisce il materiale utilizzato. Questo fenomeno ha quindi incrementato gli scenari rispetto ai quali occorre interrogarsi sull'applicazione della nozione di “partecipazione diretta alle ostilità” al personale civile così impiegato. In non pochi casi si sono registrate situazioni nelle quali i tre criteri cumulativi delineati dal CICR nelle linee-guida interpretative sul tema adottate nel 2008 potevano dirsi soddisfatti, con la conseguenza che gli Stati interessati esponevano questo personale alle possibili conseguenze negative derivanti dallo svolgimento di simili attività nello scenario conflittuale.

Per quanto concerne i proposti nuovi sistemi di arma, elemento centrale rimane a nostro avviso l'esigenza, espressa all'art. 36 del Primo protocollo addizionale, secondo cui “nello studio, messa a punto, acquisizione o adozione di una nuova arma, di nuovi mezzi o metodi di guerra... un'Alta Parte contraente ha l'obbligo di stabilire se il suo impiego non sia vietato... dalle disposizioni del presente Protocollo”. La centralità di questa disposizione e la natura delle misure che devono adottarsi per tradurre in impegni concreti questa previsione normativa sono state opportunamente ribadite, con unanime consensus, nel corso della 28a Conferenza internazionale della Croce Rossa e della Mezzaluna Rossa del 2003. In tale ambito si è sottolineata l'esigenza di adottare un approccio di tipo multidisciplinare alle problematiche sollevate dai nuovi sistemi di armamento. È quindi necessario che si dia pari rilievo a considerazioni di natura giuridica, militare e umanitaria, con uno specifico riferimento

ai possibili effetti causati sull'ambiente e sul benessere e la salute delle persone coinvolte, dando adeguato rilievo allo studio di quegli effetti sulle persone che sono meno familiari al personale sanitario. L'art. 36 determina altresì un implicito obbligo per gli Stati, talora non adeguatamente sottolineato, di dotarsi di efficaci meccanismi e strutture di revisione interna circa la conformità giuridica dei possibili nuovi sistemi di arma, di qualsiasi natura essi siano. Rispetto a questo obbligo, la puntuale "Guida" sull'implementazione di questa disposizione normativa, predisposta nel 2006 dal CICR, rappresenta un fondamentale strumento in materia.

È evidente, però, che, in molti casi, specifiche previsioni normative volte ad interdire espressamente alcuni dei nuovi sistemi di arma oggi al centro del dibattito siano difficili da rinvenire. L'evoluzione pattizia del diritto internazionale umanitario è ancora principalmente ancorata ad un'ottica di risposta normativa ex post rispetto ai concreti utilizzi e solo in pochi casi, riguardo ai sistemi di arma, è stato possibile giungere a specifiche proibizioni prima di concreti impieghi, come nel caso del primo Protocollo alla Convenzione sulle armi classiche volto a proibire le schegge non localizzabili. Per ora, non sembra che una simile possibilità sia ipotizzabile rispetto ad alcuni dei nuovi proposti sistemi di arma oggetto dell'odierna riflessione. Di conseguenza molti di questi sfuggono ad una puntuale proibizione, dato che le loro caratteristiche tecniche non corrispondono interamente alle definizioni normative basilari fornite nei principali strumenti normativi di riferimento. Rispetto a diversi nuovi sistemi di arma proposti, quindi, più difficile si presenta la valutazione giuridica, con la possibilità di arrivare a soluzioni interpretative non univoche.

Nondimeno i principi generali operanti in materia, quali a mero titolo di esempio il divieto dei mali superflui ed inutili o il divieto di utilizzo di armi di natura indiscriminata, possono fornire utili elementi di riflessione onde valutare la legittimità dei nuovi sistemi di arma e, non ultimo, la stessa residuale applicazione della clausola Martens, che la Corte internazionale di giustizia ha nel 1996 autorevolmente riconosciuto quale "un utile strumento per fronteggiare la rapida evoluzione della tecnologia militare", deve orientare le soluzioni interpretative verso l'applicazione di un principio di precauzione da applicarsi necessariamente nei casi dubbi.

Se poi vogliamo estendere la nostra riflessione all'ambito della responsabilità internazionale possiamo chiaramente vedere come molti di questi sviluppi tecnologici determinino degli scenari particolarmente complessi, che dovranno comunque essere adeguatamente affrontati. Basti pensare alle difficoltà di attribuzione ad uno Stato di eventuali condotte illecite connesse ad episodi di cyber warfare, dato che i comuni principi applicabili in materia trovano una difficile trasposizione in questo

ambito. Simili problematiche possono presentarsi anche nell'ambito della definizione della responsabilità penale individuale, date le ovvie incertezze nel definire questa tematica in alcuni degli scenari ormai prospettati dalle nuove tecnologie, come nel caso di utilizzo di strumenti bellici da postazioni remote, dove tra l'altro si assiste alla compartecipazione di più attori nella produzione del possibile evento bellico illecito.

In conclusione, sono quindi certo che i lavori della presente Tavola Rotonda permetteranno di approfondire le complesse tematiche in oggetto dell'impatto delle tecnologie sull'applicazione del diritto umanitario e, pertanto, ringrazio nuovamente l'Istituto per aver permesso la realizzazione di questo rilevante consesso, dal quale ci auguriamo possano venire proposte concrete per ottenere un maggior rispetto del diritto umanitario.

II. Legal and operational impact of technology on modern warfare

Setting the scene: new challenges for IHL

Michael Bothe

Professor of Public Law, Johann Wolfgang Goethe Universität,
Frankfurt am Main; Member, IIHL

1. Prelude: the controversy about the crossbow

New technologies and warfare are companions. Throughout history, new technology, once developed, has soon been used for purposes of warfare, and a desire for arms superiority over supposed enemies has prompted many a technological development. Over the centuries, this has sometimes been accompanied by legal question marks. A ban on the crossbow as being an inhumane weapon was issued by two popes and one church council (the Second Lateran Council of 1139). The discourse was humanitarian and theological; the reason behind it was the fact that the invention of the crossbow put into question the traditional form of warfare: the knights' armour did not provide protection against crossbow arrows, that new invention thus challenged the belligerent privilege of the knights. That ban on a new technology was, however, never really implemented, new types of weapons and warfare develop unhindered by legal or moral constraints.

Are current attempts to hedge the use of new technologies in warfare something like the fight against the crossbow? The answer to this question lies in the response to a more fundamental question: does the law of armed conflict as it has gained shape over the last two hundred and fifty years protect outdated privileges, or is there a different type of essential value which is challenged by new technologies but which deserves to be preserved?

2. Essentials under stress: the principle of distinction in the context of changing conditions

The fundamental and essential principle governing the law of armed conflict for the last 250 years is the principle of distinction, to which the protection of fighters who are *hors de combat* and the prohibition of

causing unnecessary suffering are ancillary. It is based on the concept, developed by Jean-Jacques Rousseau in his *Contrat social* of 1762, that war is a conflict between sovereigns, and limited to engaging their respective military efforts against each other. By thus limiting the group of persons entitled to take actively part in hostilities (combatants) and the scope of persons and things passively affected by them (military objectives), it establishes a far reaching restraint on military violence. Founded by Rousseau as a command of reason, it also had a basis in the reality of the wars taking place in Europe in his time, the so-called cabinet wars.

Contrary to what happened to the ban on the crossbow, this principle survived the disappearance of the military concepts which had surrounded its creation – although these changes in the military context put the principle under serious stress. Just to mention two major challenges to the principle: the development of military aviation and the invention of the atomic bomb. The former allowed extending military action well beyond what used to be called the enemy lines and exposed the civilian population in an unprecedented way to the dangers of hostilities. The latter, by its unprecedented yield of kinetic energy, heat and radiation, facilitates massive attacks where the distinction between civilians and civilian objects on the one hand and military objectives on the other is no longer feasible. Yet the legal principle of distinction has survived these challenges. Soon after the Second World War where this principle had come under such serious stress, a legal and political discourse developed throughout the world maintaining the principle of distinction against this challenge. The judgments of the Military Tribunals established after the war, the so-called Delhi Rules elaborated by the ICRC in 1956, the provisions of the 1977 Additional Protocols on the protection of the civilian population, military manuals nowadays governing the behaviour of many armed forces, and last but not least the Advisory Opinion of the ICJ (International Court of Justice) on the illegality of the use or threat of use of nuclear weapons are the highlights of this discourse which has effectively upheld the principle of distinction.

That resistance of the old principle against the challenges of modern technology may look like a miracle – but it is not. It is firmly grounded in a social and political reality, namely in value convictions prevailing in the international community. These convictions consider the principle as the necessary cornerstone of the protection of the human person even in times of armed conflict, a cornerstone which for the sake of the human person may not be given up.

3. The challenges of new technologies – a summary

During the present symposium, the science and science fiction element of modern warfare technology will be explained in greater detail. But in order to elucidate some legal problems, a simplifying summary must be given first. The basic technological innovation we have to deal with is a mixture of computer, space and telecommunication technologies:

- The dependence of both the military and civilian life on computer technology and in particular computer networks does not only create new opportunities, it also leads to a new vulnerability. Putting these computer systems out of action or causing their malfunction can constitute damage as serious as physical destruction, both for the military and for the civilian side. As a consequence, electronic attacks in various forms (e.g. infecting computers with viruses, worms, trojans) constitute a new type of acts harmful to the enemy.
- Computer, space and telecommunications technology provides new opportunities for long distance, tele-guided attacks. They facilitate a high degree of automation of attacks (e.g. the use of robots) which have a great potential to reduce the attackers risk of casualties.
- Computer, space and telecommunications technology provides unprecedented opportunities for collecting, digesting and distributing information. This is an opportunity which can and must be used for taking precautionary measures, making sure that attacks are only directed against military objectives and that excessive civilian damages are avoided. On the other hand, the reliability of the relevant information thus collected and used is often questionable.

4. The principle of distinction – still an appropriate yardstick?

The essential question we have now to answer is the following: do the customary legal rules protecting the civilian population, i.e. the essence of the principle of distinction, provide adequate legal guidance for the use and non-use of these technologies? I will try to answer this question by browsing through the major relevant rules.

5. The action: new forms of attacks, so-called cyber warfare

The first question arising is that of the object of the rules: AP I speaks of “attacks” which are prohibited or not, and this means, first of all, causing physical destruction of objects or bodily harm to persons. But are the rules limited to this kind of violent action? As to military objectives, energy transmission lines and telecommunication systems have always been considered as such because their use was essential for military action. Is there a difference in military significance between their physical

destruction and depriving the military of their use by placing a worm into their computer system?

As to the damage to civilian life, there are clear indications in AP I that the harm to be avoided goes beyond physical destruction or immediate bodily harm. “Starvation” of the civilian population is prohibited. For that reason, the destruction of means essential for the survival of the population is prohibited “*for the purpose of denying them for their sustenance value to the civilian population*”. Similarly, Art. 55 prohibits the use of methods and means of warfare which may endanger “*the health or survival of the population*”. All this points to the rationale underlying the rules on the protection of the civilian population: they are not only concerned with physical destruction, but with preserving a minimum of living conditions for the civilian population. Any action which destroys or seriously damages the living conditions of the civilian population even without involving physical destruction is covered by the prohibitions protecting the civilian population. This is essential for an assessment of so-called cyber attacks.

6. The actors: combatants and hackers

There is a high probability that such “attacks” are not, or at least not only, performed by members of the armed forces, who are combatants, but also by civilians acting with or without a mandate given by a State. It lies in the consequence of the interpretation of “attacks” just developed that the hacker is a civilian taking “a direct part in hostilities”, i.e. loses his or her civilian immunity. In the light of the developing technology of targeted killing, this involves a serious risk.

7. The target: military objectives in the light of technological developments

In the light of the military significance of computer networks, many of them are military objectives, be they used by the military only, be they dual use networks. They may be attacked by electronic means, for instance, by infesting them with viruses, but the physical components of the networks, e.g. servers, may also be attacked.

The essential question which remains to be answered is what type of network constitutes a military objective? This qualification certainly applies to networks used by the Ministry of Defence or by an army to transmit relevant information to those actually fighting, for instance, designating targets in air warfare. But what about networks used for financial transactions of the military, in particular where this is a dual use network? Or is even the entire financial transaction system of a State (which could be shut down by a hacker) because of its military significance

a military target – including, for instance, the computer centre of the Deutsche Bank in Eschborn near Frankfurt?

8. *The target: the new vulnerability of a computer-dependent society – new dimensions of the principle of proportionality?*

The dependence of life in modern civilization on an infrastructure relying on computer system involves a high degree of vulnerability. That vulnerability must in particular be taken into account when it comes to the application of the principle of proportionality. Shutting down computer systems may yield a high military advantage, but the risk of damage to the essential living conditions of the civilian population is also very high. This must be put on the civilian side on what is called the proportionality equation.

9. *Targeting: precautions in preparing attacks*

It has been shown that new technologies create new risks for the victims of armed conflicts, but there are also potential benefits. Modern technology provides unprecedented opportunities to collect and transmit information. This is *inter alia* essential for the precautions which have to be taken in the preparation of attacks. Those deciding on an attack “shall do” “everything *feasible* to verify that the objectives to be attacked are neither civilian nor civilian objects”. They shall take “all feasible precautions in the choice of methods and means of attack with a view to avoiding... incidental loss of civilian life...”. The feasibility of such precautions has been greatly increased by modern technology. “*All feasible* precautions” means that a party having these possibilities must use them.

Not only in its own interest, but as a necessary part of obligatory precautionary measures, a party to a conflict must protect its information retrieval systems against outside manipulation and must make every feasible effort to ensure the reliability of relevant information.

These principles apply regardless of the technology which is used for attacking. They are of particular importance in the case of long distance, television-guided or automatically guided attacks. In the latter case, part of the decision-making in conducting an attack is delegated to a computer programme. The duty to take precautionary measures means in this case that the relevant data concerning target acquisition are fed into the programme to the effect that the principle of distinction is respected.

10. *Essentials to be preserved*

Playing science fiction in warfare involves a high temptation of concentrating on military advantages to be gained and to neglect the

basic principle of distinction which preserves the protection of the civilian population. Rousseau, 250 years ago, laid the basis for this principle as a rule of reason. As such, it has withstood serious challenges because of its primordial importance for the protection of the human person. The basic rationale of modern law of armed conflict must not be forgotten when more modern technologies are introduced into modern warfare. A sound interpretation of existing law can indeed maintain the principle when we deal with developments of modern warfare which for some of us may be regarded as science fiction. The principle of distinction is not old-fashioned, it must not be modified, it can and must be applied in an appropriate way.

This should be the message of the present symposium.

New technologies: science fiction or real world?

Theresa Hitchens

Director, United Nations Institute for Disarmament Research, Geneva

I was asked to talk about whether new technologies were considered science fiction or a reality and I got very excited when I heard this because I am a big fan of science fiction actually. However, it is a very broad topic and, besides, the two focuses that you have here today and the next days are robotics and cyber warfare, so I thought I'd mention that there are other areas of new technology that are really, really interesting for the future of warfare. I am just going to throw a couple out quickly. They are not in my talk but I started thinking about far out things, like nanotechnologies and synthetic biology and what you could do in a world of war craft-type scenario with those kinds of things. Maybe, you will have a follow up conference looking at really far out science fiction technologies to see what you ought to be thinking about it in a very far future. But, anyway, I was forced to bring myself down to earth so as to limit the discussion, so I decided I was going to talk primarily about space and cyber as the new frontiers for war fighting.

The reason I chose those two arenas is because both realms have become the focus of growing international concerns. You are starting to see a lot of discussion at a multilateral level about how to deal with the potential for conflict in these two arenas. These choices are also similar in that they are largely commercial and civil domains, but the use of these technologies provides unique military advantages during wartime. Almost 100% of the technologies are dual use and you have a problem in that a defensive act is often the same thing as an offensive attack. In other words, the technology can be used for either thing. It does not know whether it is offensive or defensive. It is the same technology. And there is military R&D actively underway for the use of both of these domains in an offensive manner.

I am going to start with space weapons related issues. As you heard in my introduction, this is something I have had some experience in, and

I spent pretty much the last eight or nine years working on questions of space security so this is a topic that is near to my heart. What I wanted to do is go over what we are talking about when we talk about space weapons. There are three big categories of space weapons that are theoretically possible: there are weapons that are based on Earth that are designed to shoot down space systems on orbit; there are weapons based in space designed to shoot down other things in space like satellites; and then there are space-to-Earth weapons, weapons based in space, designed to hit targets on the ground. There are essentially three types of destructive technologies that are possible for these various kinds of systems and that is: kinetic energy, which is hit to kill – it does not use explosives; explosives -- conventional explosives, nuclear explosives; and directed energy, which are either lasers or high powered microwaves.

If we start with Earth-to-space weapons, what are we talking about? We are talking about ground-, air- or sea-based, anti-satellite missiles. Generally, you are looking at kinetic energy, explosives or perhaps high powered microwaves, but mostly kinetic energy and explosive type weapons. These weapons are here today: they are feasible, they are affordable and they have been tested. Anyone with a medium-range ballistic missile and a reasonable amount of technology, perhaps a satellite on orbit, can build an anti-satellite weapon (ASAT) and launch it. Another type of ASAT is also launched from the Earth, but it is put into orbit around its satellite target. These can also be kinetic energy, explosives or high powered microwave. There are some disadvantages to this technology. Such an ASAT would require a very large launcher. You have to deploy it in advance. In other words, it has to be sitting up there, ready for use when you go to war or when you decide to attack, which means it could be degraded: it could be hit by a space debris, it could lose power, things like that. They are expensive and they are vulnerable because they are big and you can see them, so somebody else might target your weapon that is based there. The Soviets tested this kind of system unsuccessfully and they never did deploy it.

Then we get to space-to-space weapons. One of the big things that's been very controversial for many years now, since the 1980s and the Presidency of Ronald Reagan, is the question of space-based ballistic missile defence and the possibility that such a system could also be used for offence. You are talking about kinetic energy again here. Such systems also require advanced deployment, but really the big problem is the fact that you have to have multiple numbers of these weapons on orbit to make the entire system work and work reliably. That means putting lots and lots of mass into orbit, which is incredibly expensive. It is not cheap to put stuff

into space. So as a result, despite of an off and on love affair with the idea of space-based ballistic missile defence in the United States, you really see very little money and real research put into that, because you run up against this wall – not the violation of the laws of physics, but the limits of engineering and the limits of costs.

The other weapon that is often talked about in the popular press (and you see lots of pictures of the thing) is the space-based laser, which, if you had something like that based in space, you could also use as a space-to-earth weapon potentially. But this is science fiction. It is science fiction for the foreseeable future. It simply requires too much mass to orbit because of the large amounts of chemicals that you currently need to pack into a high powered laser. It is just not feasible. It is not possible and it is also not worth it for the cost-benefit ratio because you actually have a very small area that you can target. You are talking about having a very small beam to be effective, so it is not exactly a cost-effective weapon, even if the costs were half or a quarter or an eighth of what the costs would be today. So, when you hear about space-based lasers being developed, do not believe it. They are not happening any time soon.

So, what about space-to-Earth weapons? Ok, this is the most fun idea in a lot of ways, the one that is often called rods from God. It has been floating around in Air Force PowerPoint charts, a little fancier than the one I have today, since the early 1990s. This is also science fiction and even more so than the space-based lasers. You are really talking about pushing the limits of engineering and materials science. You are talking about vast tonnage; trying to get vast tons of things into orbit. You have got materials issues with trying to get these things down through the atmosphere without it ablating, in other words, without losing their shape. You would have to put up these things in a big, giant “Mother Ship”. Essentially the system is composed of titanium rods that would be designed to ram into their targets on the ground at a very high speed, but you would have to base them in this big Mother Ship with hundreds of these things based there. And the platform itself becomes a highly vulnerable target, something somebody could shoot with a cheap ASAT, the first type of weapon I talked about. So, it does not make any sense from any perspective whatsoever and it would also be outrageously expensive. So, whenever you see these old PowerPoints floating around, remember that they are just that: PowerPoints. I don't think that one dime was actually spent on this research. It was only ever a piece of paper.

The other things that have recently been in the press, because of the amount of testing going on, again mostly in the United States, are hypersonic space planes. These use special engines called scram jets,

air breathing jets, to boost into orbit and this technology is actually not science fiction. It is in the early stages of testing. There have been a number of tests in the United States. You can see them here on the PowerPoint slide. This technology is still pretty expensive and again you are talking about very early days of demonstration technology. There was a lot of kerfuffle about the USAF X-37B, the secret space-plane demonstrator. People have been speculating: this is a weapon. But it is really small. It does not have a big payload bay and I pretty much doubt that it is carrying ordinance. This is my guess (and probably the best guess of people who do not have security clearances): It is a kind of intelligence gathering platform. It is really too small right now for anyone to be concerned that it will be shooting things down.

Ground –, sea – and air-based ASAT and kinetic ASAT are here today. They are proven, missiles are widely available and the only hard part for would-be ASAT owners is gaining targeting capabilities. That is actually the hard part, the targeting of the satellite, keeping your ASAT aimed at the satellite, which, remember, is not in one place, but moving very fast. So that is the difficult thing, but it is not out of the realm of the possible for anyone with a space programme and medium-range ballistic missiles. I can tell you that India has been looking into that quite seriously since the Chinese ASAT tests in 2007.

Space-based weapons of any sort are not likely in the near term. They are just not. The hypersonic space planes are the most feasible, but, as I mentioned, the rest are just science fiction. They are fun to read about and they are kind of cool when you look at the models but they are not coming any time soon. Do not worry about regulating them or applying international humanitarian law to them.

Now I am going to move to cyber weapons, quickly, because I am running out of time and you will have a whole session on this later in the conference, so I will be short. The cyber issue worries me actually as much as the space issue. Remember these two things are related. The Internet works via satellites. Yes, some of Internet traffic goes through cable, but a lot of your telecommunications, whether it is via the ‘Net, whether it is telephone calls, broadcast, television, video, it all goes through satellites. You touch a satellite everyday: when you go to get money out of the bank from your ATM machine; most of the time when you get on the ‘Net; when you turn on the TV. Space technologies are an enabling technology for cyber communications. So, they are related things.

Sadly, there are all sorts of cyber attacks going on right now. The computer security firm, Symantec, just put out a study pretty recently saying that there were 286 million attacks in 2010, a 93% increase from

2009, and the biggest increase in the types of attack was in the use of social networks, like Facebook, as a vector for the virus, or the worm or the malware.

Cyber activities are easily adapted for use in war fighting and you have a real question here about how to characterize what is an actual attack. So, I took the example of the Stuxnet worm which I am sure most of you will have heard about, which was targeted against Iranian nuclear reactors. If somebody had blown up these reactors, that would have been a legitimate act of war. True or false? It is a good question.

The barriers to entry for cyber war are low. You only need a computer and a brain. I will tell you a story: my son at the end of last year, he was sixteen years old, he and two of his little buddies got in trouble on the last day of school for hacking the school computers system and putting up jokes on the front page. He is by no means a computer whiz. Better than me, but not a genius. So, a computer and a brain.

As you heard earlier, attribution is also an issue. There are some countries that are better off. Again, my home country made a lot of progress with this, but it is a real problem. There is a further difference between technical attribution, that is, I know where this is coming from – and political attribution. It is the same thing in satellite jamming. Right now we have had an issue where jamming has been coming out of the Iran against EUTELSAT satellites that started just before the Iranian elections. The ITU, the International Telecommunication Union, has pinpointed where that jamming is coming from, but Iran has denied that they were doing it (that the government is doing it) and they said they cannot do anything about it. So, that is the difference between technical attribution and political attribution; and that is true in the cyber realm too, where you have, for example, these patriotic hackers who, the Chinese Government, the Russian Government and whoever where this has been happening, have denied that they have anything to do with, and they may well not, but you have no way of proving whether these are hired guns or whether they are doing it on their own.

The only bright ray in the cyber arena is that protection is getting better, so the offence-defence cycles are really fast and that is actually a good thing. So probably the playing field has been keeping relatively even.

Here are some types of cyber weapons I am going to go over really quickly: viruses, which are attached to a programme and replicated into the system; worms, which are stand-alone viruses; denial of service attacks, think about Estonia; some things that are called Trojans or rootkits, which are kinds of backdoor programmes that are designed to infiltrate a computer, steal the data and then open a pathway, a backdoor,

into your computer so they can keep stealing data and they can avoid your security systems; botnets, that probably everybody will have heard of, sort of zombify the computer and take it over to do the job of the botnet without the owner's knowledge. You will have a sort of master control person who is controlling all these botnets, and these systems can be huge, I mean really huge, and they can do all kinds of things: spy, steal data, spam, and launch attacks in cover identities. In fact there is a really big business on the black market in crime in using botnets. Cyber criminals are known to rent out their botnets for certain activities to other entities.

Some thirty-six countries have on-going cyber defence activities that actively involve the military. Some ten to twelve countries are thought to be incorporating offensive cyber activities into their doctrines, if they have not already done so in their actual activities. Although, I would say that I think stand-alone cyber attacks are unlikely. There is a lot of hype about this – the supposed cyber bolt from the blue: that is, somehow somebody is going to come out of nowhere and is going to turn off everybody's water systems and dams, etc. in one fell swoop. I think this is not likely, it is not politically likely. It might be physically possible, but it is not politically likely. I think that cyber attacks are likely to be incorporated in an overall war fighting strategy. It might be the first go, but it is not likely to be something that is out of the blue.

The conclusions regarding the cyber realm are: be afraid! The pace of development of malicious code is a challenge for security, especially for lumbering bureaucracies. Bureaucracy moves slow and remember I said the action-reaction circle of the creation of viruses and bad malicious code and defence is quite quick. It is quick in the commercial realm, but not in the governmental realm, which is a problem. I said be afraid, but not yet *very* afraid. So, do not panic! Most attacks that have happened up to now are cyber crime, followed by cyber espionage and you know that is one of the oldest professions. So far, we have seen no activity with the possible exception of Stuxnet, that can conclusively be said to comprise use of a weapon nor have we seen the use of cyber attack as a war fighting tool – again with the possible exception of the conflict in Georgia. I say possible exception in both of these cases because the jury is out on how to judge these activities.

My “concluding conclusions” are that there are current threats to international security from new and evolving technologies in space and cyber. There are threats today and those are threats that we need to deal with. And I am afraid that the international community, the legal community, is behind the power curve, because those weapons are there

and ideas on how to use them are there. International law, in particular, has not caught up with these threats, which is why we are having this conference. Lastly, as a piece of advice, do not panic until panic is due. There is also a lot of “science fiction” thinking and hype about how difficult these threats are to counter and what “drivers” exist to use such weapons. It is early days, we still have time. We may be at the end of the power curve, but we are not so far behind the power curve that we need to panic. What we really need is for the multinational community to sit down collectively and try to deal with the question of how we can constrain the abuse and misuse of these domains.

Impact on military strategy, capability development and doctrine

Erwin Dahinden

Director, International Relations, Swiss Armed Forces, Bern;
Council Member, IIHL

The purpose of this contribution¹ is to provide an overview of the implications for the politico-military level and force planners. It may be helpful to better understand how the military try to carry out the political mission. In reaction to threats, they build up a potential of weapons, a doctrine how to use them and procedures to guide and control their use. All these elements have an influence on the way International Humanitarian Law can be implemented and what consequences and impediments one has to face in the political process.

There is a well-known saying that the “military always prepare for the last war that has taken place”. Moreover, looking at recent history, one can augment this quotation with “... the diplomats try to prevent the last war and the politicians tend to ignore the last war”.

These quotations bear some truth as far as they show that we are all selective in our views on history. Moreover, we may ignore current developments and even be blind to the emerging contours of the future. Dealing with military strategy and force planning you may be influenced by historical experience, but you depend on political guidance and resources restraints, and your military preparation and war fighting capabilities should be oriented to present and future needs. You have to face the uncertainties of enemy capabilities and behaviour.

1. This paper presents my personal view and does not necessarily reflect the official Swiss stance. I would like to thank the following colleagues for their valuable support in the preparation of the seminar: Col GS Alain Vuitel (charts), Col GS Claude Meier (military doctrine; UAV), Dr. Peter Baltes (military economy), Dr. Mauro Mantovani (UAV) and Col GS Gérald Vernez (cyber defence).

1. Strategic context

New technologies and innovations play an important role at the political level. They are some of the most important growth factors of national economies. They promise a high return on investment, improve competitiveness in global markets and attract the best minds for research and development. In the mind of politicians, new technologies and innovations are also part of national prestige and able to improve future economic and military power. However, there are some inherent dangers with new technologies and innovations. Because of their large potential and prestige, some negative implications of new technologies might be discounted or even outrightly denied. Current pressing problems might be ignored hoping that they disappear as new technologies become reality and higher risks might be incurred. Such considerations apply to both civilian and military technologies and innovations. However, new technologies are tools or instruments but not solutions in themselves.

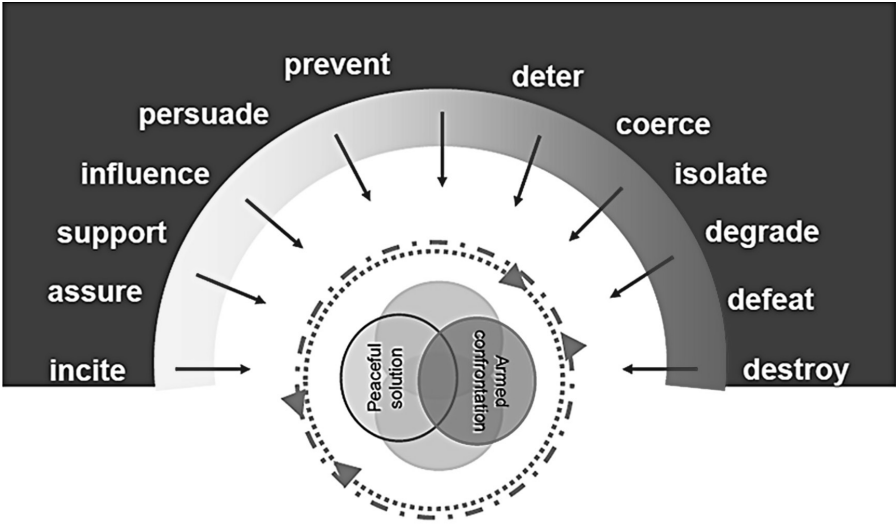
There are important synergies between military and civilian technologies. On the one hand, military technology is in many ways related to the technological development of national societies as such². On the other, specific military needs such as miniaturisation of electronic components (computer chips, mobile communications devices), resilient communications networks or new materials have led to technological breakthroughs in the civilian world (personal computers, Internet). Sometimes, it was the military application of civilian expertise and in other areas military needs that mobilised research and knowhow that also had an important impact on the civilian world. “The way you earn your wealth you fight your wars”.

The main political incentives to improve the technical level of armed forces can be summarised as follows:

- in times of war, the introduction of new weapon systems improve the likelihood of success/effectiveness of military operations;
- to improve flexibility and utility;
- to strengthen military power projection and deterrence;
- to reduce the size and the (total) costs of the armed forces.

In particular, advanced technology improves targeting and precision of military strikes, which from a military point of view have some important advantages such as the high probability that the target will be properly identified and destroyed, the minimization of collateral damage and a better implementation of humanitarian obligations regarding criteria of

2. See Toffler Alvin, Toffler Heidi, *War and Anti-War. Survival at the Dawn of the 21st Century*, Boston 1993.



Graph 1 - Modern tasks of armed forces

distinction. The perspective of a more precise weaponry and better effectiveness of military strikes also offers, in what are referred to as post heroic societies³, the significant political advantage of using the armed forces with fewer risks to the lives of soldiers.

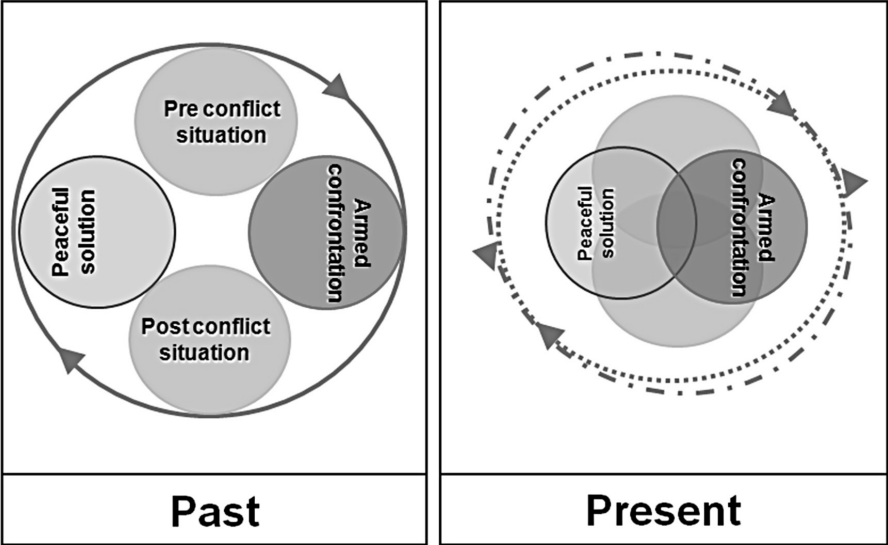
First, this might facilitate the willingness to engage military means for specific political objectives (e.g. anti-terrorism) and make military attacks more acceptable to the public. Recent discussions on modern warfare seem to suggest that military technology and innovations may lower the threshold that currently limits a state's military action. Military action or war may become the most preferred option rather than the last resort of foreign policy. At the level of the individual soldier, advanced military technology may strengthen his motivation and improve what is known as force protection.

Second, there may be a counter-effect to the lowering of the threshold: During the Cold War the technological improvement of nuclear strategic and tactical forces was essential for preserving the credibility of Mutual Assured Destruction (MAD) as a strategic concept. With respect to conventional forces, advanced military technology may have an important deterring effect. The current technological superiority of Western military

3. See Muenkler Herfried, *Der Wandel des Krieges*, Göttingen 2006, p. 310 ff.

forces could be so overwhelming that asymmetrical warfare might become the fighting strategy of choice for the technologically less advanced military forces of developing countries. This is a thesis the Chinese Colonels Qiao Liang and Wang Xiangsui propose in their book *War beyond limits*⁴. They see technological dominance as the main incentive for asymmetric warfare⁵ and identify among others economic warfare and cyber warfare as valid alternatives. In short, the introduction of new weapon systems may increase the superiority *ex ante* (lowering the anticipated costs of conflict for the conventional force). In reaction, the opposition changes the rules of the game by fighting an asymmetric war that, as recent experiences prove, increases the costs for the intervening force.

There is an on-going discussion among military experts as to whether the armed forces only have to provide a victory to form the decisive basis for a political and diplomatic solution (end state)⁶. This position is very much contested by recent experience where the armed forces have had to provide security among people, as indicated by General Rupert Smith in his book on the utility of armed forces in modern warfare⁷.



Graph 2 - Changing nature of conflicts

4. See Qiao Liang, Wang Xiangsui, *La Guerre hors limites*, Paris 2006, p. 250 ff.

5. Who is fighting the future wars is also relevant. See Van Creveld Martin, *The Transformation of War*, New York 2009.

6. See Rose Gideon, *How Wars End*, New York, London, Toronto, Sydney 2010.

7. Smith Rupert, *The Utility of Force*, London 2005, p. 267 ff.

Not the capability to destroy, but to use appropriate force and to differentiate between innocent civilians and combatants is seen as a precondition for the legitimacy of the use of armed forces and an important tool for the political solution of a conflict. Either you defend your own territory independently or you are engaged in an out-of-area crisis management mission. The well-known catchword to win “hearts and minds” becomes the basic guideline for a military engagement on the ground along with the creation of a favourable framework for reconciliation and state building. As a consequence, equipment, training and the use of force must be appropriate for such a mission⁸.

As an intervention on the basis of a UNSC mandate is legitimised through the defence of fundamental rights and values (protection of the population, R2P), the use of force during that mission must also be limited to the restrictions inherent in the same values⁹. Although new technologies may improve capabilities at the military-strategic level and even facilitate the subordination of military goals to political ends, there is also a great danger that advanced military technology becomes an end in itself and induces politicians to take higher political risks.

In conclusion, it should be pointed out that strategy has a “bridging” function¹⁰ linking the political goals with the resources. Thus, a continuous dialogue is needed between political levels to promote mutual understanding and to reduce the risk of surprise for all levels. Technological supremacy cannot replace strategic and political soundness.

2. Technology and military capability

Available technologies have always been used by the military to improve the performance of existing weapon components (superiority versus denial). Any technological advance has triggered efforts to deny military advantages. This technological arms race has been a continuous process since the beginning of civilization¹¹.

The potential of new technologies has seldom been identified from the beginning: e.g. tanks were used in WW I to enforce infantry, and aircraft was deployed to gather intelligence and support artillery. It was the Italian

8. See Desportes Vincent, *Penser Autrement, La Guerre Probable*, Paris 2007.

9. Compare Kilcullen David, *The Accidental Guerrilla, Fighting Small Wars in the Midst of a Big One*, Oxford 2009, p. 109 ff.

10. See Gray Colin S., *The Strategy Bridge, Theory for Practice*, London/New York 2010.

11. See Boot Max, *War Made New, Technology, Warfare, and the Course of History, 1500 to Today*, London 2006.

General Giulio Douhet who transposed concepts of naval warfare to the air and in his work *Domination of the Air* of 1921 developed the role of the air force in claiming “to have command of the air is to have victory”. In WW II, General Guderian used the speed and weaponry of tanks and aircraft to launch deep strikes and to develop them as independent branches (concept of tanks as shields and aircraft as swords).

Technology and sophisticated weaponry alone do not guarantee military success. Other key factors that must be present are leadership (General Patton), skills, resilience and logistics.

The motivation to replace soldiers by technology is understandable because of overall costs, vulnerability and political implications. Battle experience repeatedly corrected this aspiration, e.g. in the 2006 Lebanon war, where failures were provoked by the overestimation of technical intelligence and the lack of HUMINT. The concept of relying mainly on air forces and Special Forces for intervention, the so-called Rumsfeld Doctrine, failed to meet expectations in ENDURING FREEDOM in Afghanistan.

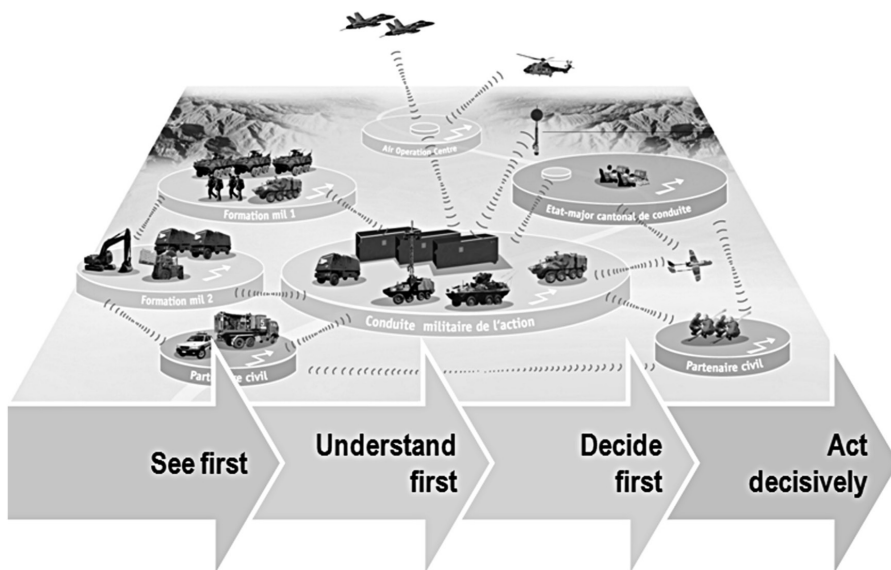
The technological sophistication of military means is also an important element that enhances the morale and self-control of a soldier. The more confidence soldiers have in the effectiveness of their kits, the better their discipline and, as a consequence, their observance of the Rules of Engagement (ROE).

3. New capabilities and force structure

“Revolution in Military Affairs” (RMA) became a catchword at the end of the 20th century. The term was originally coined by the Soviet military establishment and subsequently adopted by Israel and the United States¹². In essence, RMA gave soldiers more information about battle space, more precise data on potential targets and ensured better concentration of fire power in time and space (see graph). These improved capabilities are often summarised with the term “network enabled operations” (NEO).

NEO was first tested on a larger scale in the 1st Gulf War with impressive results. NEO requires optimum integration of the various systems and becomes what is called the “system of the systems”. This had important consequences on force planning, interoperability, upgrading and long-term financial obligations.

12. Henrotin Joseph, *La technologie militaire en question, le cas américain*, Paris 2008.

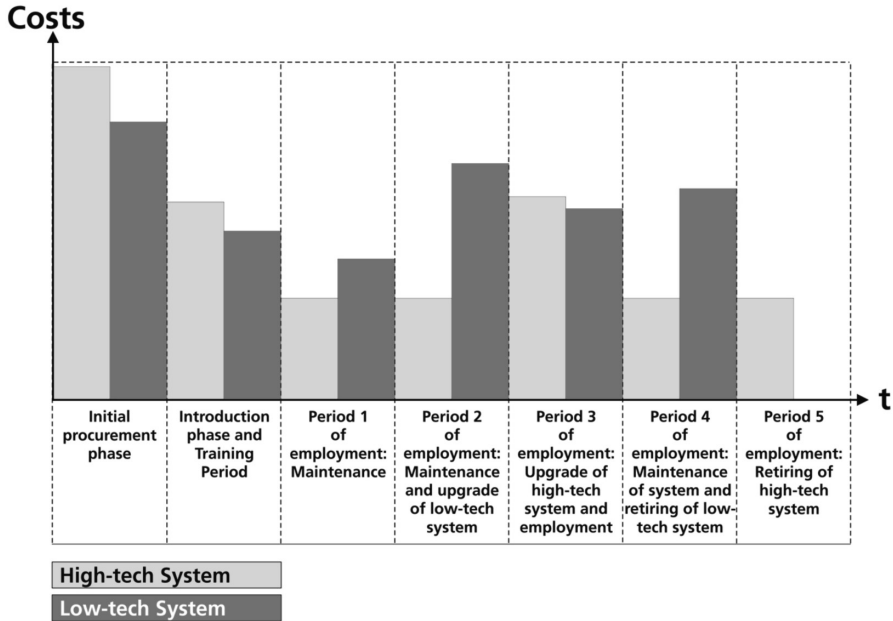


Graph 3 - Network Enabled Operations (NEO)

New technologies have fundamentally changed the planning process of armed forces, made the procurement process more challenging and extended the long-term consequences for budgeting. Given the complex and rapidly evolving nature of military technologies, maintenance and logistic support of armed forces are changing substantially: upgrades have to be realised in harmony with other users requiring international synchronisation too. Repair consists mostly of exchanging components and it is necessary to engage more civilian capabilities in the rear area or in operational logistics¹³.

Procurement was always a long-term exercise from the definition of requirements to the development of prototypes, testing and finally fielding with training. This took 10-15 years plus 20-30 years of operational use. The military call this “long-term life cycle management”. As the following graphical representation illustrates, the main costs encompass not only the actual procurement costs of a new weapon system, but have to include those occurring during its operationalisation, maintenance, and upgrading. These important long-term investments demand that the legal and budgetary framework for armed forces is highly predictable.

13. See O’Hanlon Michael E., *The Science of War, Defense Budgeting, Military Technology, Logistics, and Combat Outcomes*, Princeton and Oxford 2009.



Graph 4 - Costs

4. Doctrine

Forces have to be designed and trained for fundamentally different types of operations. This requires flexibility in their structure, their command and control and their training.

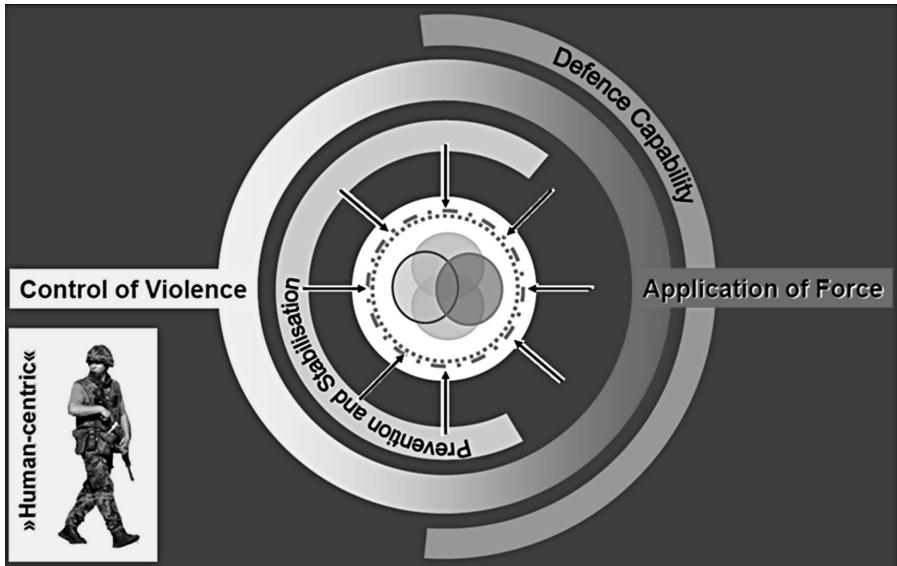
In this environment the political and military control of the use of force and escalation becomes critical and necessitates new instruments. The development of rules of engagement¹⁴ for the specific mission should be seen against this background.

The need for command and control and technical resources should not undermine mission-type responsibility which is a crucial element for the appropriate use of force in a given context. There seems to be a major weakness with technological systems that reduces reality to a certain number of sensors and regulated scenarios¹⁵.

14. See Mandsager Dennis, *Sanremo Handbook on the Rules of Engagement*, International Institute of Humanitarian Law, Sanremo, 2009.

15. See Singer Peter Warren, *Wired for War, The Robotics Revolution and Conflict in the Twenty-first Century*, New York 2009, p. 344 ff.

For a long time, a majority of military leaders thought that soldiers who have been trained for high intensity warfare were also able to carry out stabilisation tasks and that they were capable of conducting what was known as the “three-block war”. Recent experience underlines not only the need for different equipment, but also specific training and the mind-set for such missions¹⁶. Once again, fissured concepts may jeopardise proper execution of the mission.



Graph 5 - Balanced capabilities

Neither doctrine nor ROE can reduce command responsibility: individual assessment and human factors are even more important in the complex and changing environment of military operations.

5. Perspectives

The new technological capabilities have also created new vulnerabilities which were almost underestimated at the beginning of the process. The

16. Compare Grossman Dave, *On Killing, The Psychological Cost of Learning to Kill in War and Society*, New York 1995.

necessary protection measures may outweigh the expected advantages and certain systems may become “obsolete”. Many armed forces try to improve the protection of their systems at significant additional cost.

Cost-relevant restrictions through new regulations may have to overcome a variety of obstacles because of the long-term planning of armament industries and the investments involved in research and development as well as life-cycle management in the armed forces.

“Clean and surgical” strikes or wars may be desirable for the politician and appear in the marketing folders of arms sellers but remain theoretical. Although efficiency and effectiveness of weapons have been improved, considerably “long wars” and “dirty conflicts” are widespread.

Technological developments may generate new battle spaces: land, sea, air, space and now cyberspace too. The limits of past warfare may be challenged as well as the application of existing rules. Technology as such is neither good nor bad. The use of it and the respect of the relevant fundamental principles and regulations determine its humanitarian nature.

So far, oil has been a crucial resource for fighting wars. Use of the electromagnetic spectrum may grow in importance. The parallel use of innumerable systems will create unforeseeable interactions anyway and may block the functioning of systems in a crucial moment. Geography may also become less important for the exercise of power and military operations.

The human factor may again gain in importance, as in the strategic and political setting, wars have to be conducted “amongst people” (Gen. Smith) and winning hearts and minds is more difficult with robots.

Technological supremacy may stimulate the use of more asymmetrical means.

With the new means of war and the development of information warfare, the traditional concepts of prevention and defence are challenged. New approaches are especially needed in areas where states would like to cooperate and seek to limit the destructive and dangerous actions of anonymous persons, groups and criminals.

New conflicts, new technologies: the challenge of the protection of the civilian population

Soad Shalaby

Director, Cairo Regional Center for Training on Conflict
and Peacekeeping in Africa, Cairo

We are witnessing critical times in the history of the Arab region, Africa and the world.

From the beginning of this year, the world has been experiencing popular uprisings in many countries. The numbers of the civilians who lost their lives in the course of the uprising from February to October in Libya alone may amount to ten thousand people. It is fair to assume as well that the on-going brutality of the regime in Syria will bring these numbers to double.

The people living in North Africa under dictatorship rulers for over 30 years are anxious to take their future into their hands in order to guarantee the realization of their dream: gain the rights of the people for political participation, human rights for citizens and social justice of their society. The people of Tunisia, Egypt, Libya, Syria, Bahrain and Yemen wish to establish democratic systems where free and fair elections will enable them to choose their leaders who will rule under a constitution that recognizes human rights and acknowledges the responsibility of the state toward the citizens. That is how Tunisia started uprooting dictatorship followed by Egypt, Yemen and hopefully Syria and other countries in the region.

The principle in international law is that military action should be directed only at armed forces, not at civilians who are demonstrating or exercising their right to strike or civil disobedience. This principle has been long-established and widely respected by most governments. However, it was during the last decade that this principle was being breached and flagrantly not respected by state forces and the security sector in many places in the world.

That is why the issue of the protection of civilians in armed conflict became an increasingly pressing area of concern for the international community and the United Nations Peacekeeping Missions. In modern

conflicts, civilians account for the majority of victims; in some cases, the armed actors involved have taken measures to avoid civilian casualties but have been unable to achieve this, and in other cases, those involved in violent conflicts have deliberately targeted civilian lives and livelihoods as part of their military strategy.

The issue became critical for the United Nations and was placed on the international community's agenda in 1999. The first UN Security Council Resolution 1265 was issued condemning acts of violence against civilians in conflict areas. Since that date, the Security Council has held regular meetings, generating reports and producing resolutions tackling this issue.

A framework has been established through which protection of civilians can be strengthened and the responsibility of all those involved, including states, regional organizations and non-state actors in terms of their legal obligations have been outlined. The challenges that were facing UN peacekeepers in peacekeeping missions was that their mandates had to be enforced so that they could account for the violations of International Humanitarian Law as well as guaranteeing that the thematic principles were translated into actual civilian protection in the conflict ground.

In 2005, the UN World Summit endorsed the concept of Responsibility to Protect, which affirms the responsibility of national governments to protect their civilian population and opened the possibility of international accountability for failures in this regard. At the same time the Security Council set important precedents for protection of civilians through its statements, resolutions and mandates for peace missions.

Civilian protection has become a benchmark in the evaluation of peacekeeping missions' success and effectiveness. The protection of the civilian component has also been focused on as a key provision in the planning and implementation of peacekeeping missions. The new position of Deputy Special Representative for the Secretary-General for Humanitarian Affairs which has been created has improved the coordination of civilian protection efforts among UN agencies and humanitarian NGOs.

Moreover, the General Assembly Special Committee on Peacekeeping (known as the C34) recently released a report requesting UN peace operations to design specific and comprehensive strategies for civilian protection through integrated planning.

In spite of all this international awareness, the fact that tragedies still happen is due to the lack of effective strategies to protect innocent civilians, women and children, as victims of wars and armed conflicts. There is also a lack of cohesion between political will, mandates, intentions and expectations, especially if civilian protection requires the use of force.

At the Cairo Regional Center for Training on Conflict Resolution and Peacekeeping in Africa (CCCPA), training programs focusing on the real problems facing the peacekeeping missions on protection of civilians are organized regularly. This is done to prepare military, police and civilian peacekeeping officers for the duties and obligations of protection of civilians while using examples of what has happened to civilians in Afghanistan, Iraq and now Libya. The training program includes broad and specific issues related to the protection of civilians, which includes humanitarian assistance and guarantees of human rights standards and application of International Humanitarian Law. CCCPA is a partner with IHL of Sanremo and other international and regional institutes that do capacity building in this field. This helps in standardization of training among the different institutions and creates an international awareness amongst the peacekeeping community. The African Union has also included these training courses for the forces of the regional brigades that had been trained under the African Standby Force which will be creating continental early warning systems for preventing conflicts.

Yet numerous challenges still remain in all areas of armed conflict when it comes to protecting civilians, particularly in terms of holding conflicting parties liable to their legal obligations and ensuring their compliance with their responsibility to protect. This year, we have seen the examples of Côte d'Ivoire and Libya where civilians have been exposed to severe atrocities and their protection was failing. The international community has been forced to act as a result, and in both cases we can see how complex the issue of civilian protection can become. In Africa armed conflicts usually break out within a state, different local actors who emerge compete for control and usually international intervention, with its severe implications, is not welcomed.

Regarding the Libyan crisis, deplorable developments are happening and the number of civilians who lost their lives or who suffered all kinds of humiliation and defeat are unaccounted for. The United Nations mission UNSMIL, created lately, is mandated to assist the National Transitional Council which is facing considerable challenges. But six months ago, the UN Security Council with the support of both the Arab League and EU countries was called upon to intervene to prevent a humanitarian catastrophe and to address the threat posed to international peace and security. This led to the involvement of NATO forces to enforce a no fly zone on Libyan territories. There was a mutual international consensus that NATO should do the job. But the question still exists: did it succeed in protecting the civilians? Was there anything worse to happen than what had already happened?

On 19th March 2011, NATO military forces began a series of strikes on Libya. Unfortunately, the air strikes led to a number of civilian deaths. In one terrible case in June, NATO missiles hit a residential compound belonging to a humanitarian activist, killing his pregnant wife and three of his children, aged between four and eight years old. The name of the eight year old girl who lost her life was Salaam [peace]. NATO apologized for a possible failure of weapon systems. Can the world accept such crimes against innocent women and children? In the Libyan crisis NATO has been accused of killing dozens of innocent civilians. In other countries in Africa and elsewhere where civilians have suffered similar levels of brutality under dictatorship regimes, including Yemen and Syria, the world has kept silent and took no similar measures of confronting such atrocities. Are we still worried about the civilians in conflict areas? Is it a matter of principle or is it dealt with on a case by case basis depending on the political will of the veto power states in the UNSC?

As this example shows, civilian deaths occur even in missions that are mandated by the UN and the international community to save the lives of innocent people and to protect the civilians. There is also a clear link between new weapons technology and civilian deaths, as in the tragic examples from Libya, where most of the innocent civilians were killed by drone airstrikes.

The new technology of warfare which has been used recently in Iraq, Afghanistan and now in Libya and other places has encouraged the manufacturing of drones and high level technological weapons. The errors that happened and resulted in dozens of deaths are blamed on the weapon system and not on the decisions of launching these deadly weapons. It is sometimes claimed that as technology develops, it will become easier to target precisely the impact of weapons, and, therefore, civilian loss of life and damage to property might be avoided.

Unfortunately, the reality is somewhat different. For example, in Iraq or in the Palestinian territories, very sophisticated and state-of-the-art weaponry has been used and civilian populations continue to suffer high levels of death, injury and loss of livelihood. Clearly, it seems that as technology develops it is mainly to protect military users but not to protect civilians.

In some cases, advanced technology may be used by armed forces who disregard the laws of war and their obligations to protect civilians. It can be argued that the Israeli incursion into Gaza in 2009 fell into this category. This military campaign was widely criticized by the international community as involving disproportionate use of force and causing high numbers of civilian deaths and damage to civilian property. According to the Amnesty International report into the campaign, the Israeli Defence

Forces used precision weapons to kill hundreds of civilians. Highly accurate missiles launched from helicopters or unmanned aerial vehicles (UAV)s killed civilians, including children and medical staff assisting the wounded. Sometimes, therefore, we have to consider that advancements in weaponry will be used in such a way that increased numbers of civilian deaths are inevitable. It is not enough to simply assume that civilian deaths and collateral damage will be reduced as weapons become more sophisticated.

In the rather different example of Iraq since 2003, the number of civilian deaths has been, according to one estimate, more than thirty times the number of military deaths. A large number of these deaths are attributable to aerial bombardment by pro-government forces and the international troops that support them, as well as the complexities of dealing with insurgent forces. A similar pattern of significant numbers of civilian deaths at the hands of airstrikes and other advanced weaponry has also emerged in Afghanistan. Clearly, there is a need for the international community to take action to try to understand what has gone wrong here; why have these conflicts witnessed such a high degree of civilian harm? Why do women and children always pay the price of conflicts? Is it a lack of awareness, a lack of commitment to the legal obligations to protect? Is it a consequence of warfare waged against insurgent groups who may hide their troops amongst the civilian population? Crucially, how does developing technology impact these questions? Do more effective weapons lead to more civilian deaths? Do new precision and long-range weapons capabilities allow armed forces to create large numbers of casualties while reducing the risk to the troops themselves?

This last point may be particularly relevant; one key aspect of new weapons technology seem to be the capacity for carrying out long-range attacks that preserve the lives of soldiers using the weapons. Unmanned drones are used to plant bombs, saving the lives of pilots. Long-range and precision missiles may be used to hit targets, so no “men on the ground” risk their lives. It may be that these advancements, which are obviously highly attractive to the military actors who develop and purchase such weaponry, come at the expense of civilian protection. New precision technology in aerial bombardments allows targets to be struck by planes flying above the height of any reasonable air defences, thus saving the lives of pilots. Attacks from this height are, however, less accurate, and may lead to greater civilian deaths. Equally, missiles can reach long-range targets, but often kill bystanders or other innocent civilians in the way that a targeted infantry attack would avoid.

It is these considerations which must be considered when dealing with the issue of new weapons technology; who does it benefit and why do

civilians seem, in so many cases, to be paying such a high cost? It is our responsibility to bring the principle of proportionality and accountability back onto the agenda.

All these questions should be addressed when tackling the challenges of protection of civilians. This issue needs more collaboration of all parties involved-UN bodies, host governments, policy-makers and the international community at large. Definitions and mandates need to be clarified. International Humanitarian Law and Human Rights protocols have to be respected in all conflicts and not on a case-by-case basis. Finally, the political will should be focused on saving lives and decreasing the number of loss of lives of innocent civilians, and protecting the people of the world from manmade high tech weapons.

**III. Old weapons and new technologies.
How new technologies enhance
traditional weapons and weapon systems**

Kinetic and non-kinetic energy weapons: a marriage made in heaven?

Stuart Casey-Maslen

Research Fellow, Geneva Academy of International Humanitarian Law and Human Rights, Geneva

1. Introduction: it's not just IHL!

The regulation of weapons is not a task that international humanitarian law (IHL) can successfully achieve on its own. Weapon use covers issues of *jus ad bellum* as well as *jus in bello*, and encompasses counter-terrorism and peace operations as well as traditional law enforcement, including riot control, where international human rights law has a critical role to play.

This short intervention covers specific issues of concern with respect to four “methods of warfare”: cyber attacks; the use of potentially-lethal chemical agents; the use of non-kinetic conventional weapons termed “non-lethal”; and the use of explosive weapons in populated areas.

2. Cyber attacks

There's no internationally accepted definition of either “cyber warfare” or “cyber attacks”. And words matter. Does the term cyber warfare, for example, imply that an armed conflict regulated by IHL is already in progress, or can it also be the weapon that initiates an armed conflict? The *jus ad bellum* issues are important given the position of the United States of America, as set out in its May 2011 Cyber Security Strategy:

Consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace¹.

1. US Government, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011, p. 10.

Which aggressive acts does this statement refer to? When committed by whom? Stability depends on certainty and predictability; we are a long way from this insofar as cyberspace is concerned.

What was Stuxnet? Was it a legitimate act of war? A “pre-emptive” use of the right of self-defense? An act of aggression? And would our answer as lawyers have changed if some of the more apocalyptic fears of the consequences for the nuclear reactor had proven accurate?

Cyber attacks (a term I prefer to “cyber warfare”) raise particular concerns under international law. The foreseeability of harm may be difficult, thereby rendering assessments of proportionality under both *jus ad bellum* and *jus in bello* difficult. Targeting issues, both in an attack and in any response, are also challenging (as they are, of course, with respect to any dual-use object). And attribution is particularly hard when it concerns acts in cyberspace. For instance, neither the US nor Israel has acknowledged responsibility for Stuxnet, despite widespread belief that they were behind the attack. In sum, this is an area that deserves considerable further thought.

3. Potentially-lethal chemical agents

The term “non-lethal”, when applied to weapons, is, as NATO and Bill Boothby have pointed out, respectively, an “oxymoron” and a “misnomer”. The rationale for such weapons was nonetheless to reduce human suffering. However, as both the US Department of Defense and NATO note, ‘non-lethal’ weapons:

may be used in conjunction with lethal weapon systems to enhance the latter’s effectiveness and efficiency in military operations. This shall apply across the range of military operations to include those situations where overwhelming force is used².

During the Vietnam War the irritant chemical agent CS was used ‘on a massive scale to enhance the killing power of lethal fire rather than to reduce casualties’³. A well-known, more recent case is the 2002 Moscow theatre siege in which Russian Special Forces deployed an unknown chemical, widely believed to be a derivative of fentanyl, a fast-acting

2. NATO, *NATO Policy on Non-Lethal Weapons*, Brussels 1999, and US Department of Defense Directive 3000.3 of July 1996.

3. Nick Davison, *‘Non-Lethal’ Weapons*, London 2009, p. 3.

opiate⁴. The chemical was used to render the Chechen hostage-takers unconscious prior to storming the theatre and then shooting and killing all of the hostage-takers⁵. At least 120 of the 800 hostages died as a result of exposure to the agent, whose major side effect is respiratory depression⁶.

With the muted international reaction to this use of a chemical agent, there is a fear that so-called chemical ‘incapacitants’ may be a problem in the future. Their status under the Chemical Weapons Convention when used for law enforcement purposes needs to be clarified.

4. Non-kinetic conventional weapons

As we know, Protocol IV of the Convention on Certain Conventional Weapons banned the use of blinding lasers in armed conflict. Arguments that it was “more humane” to blind rather than kill were ultimately rejected by States, perhaps for fear that these weapons would fall into the hands of armed non-State actors. It was also widely understood that being blinded on the battlefield would, in any event, often be equivalent to a death sentence.

In Afghanistan and Iraq, however, troops have been equipped with “dazzling” lasers, especially for use at checkpoints and protection of convoys. Green lasers are often used as the eye is more sensitive to green light and they are more effective in daylight. While there is no evidence that civilians have been blinded by these weapons, it is believed that additional safety features were retro-fitted to the weapons following eye damage caused to US soldiers playing with the weapons among themselves.

In addition, research is on-going into electromagnetic pulses, powers and frequencies to affect the brain and central nervous system⁷. We don’t yet know where this is going.

4. See, e.g., Theodore Stanley, “Human Immobilization: Is the Experience in Moscow just the Beginning?”, *European Journal of Anaesthesiology*, Vol. 20, No. 6 (2003), pp. 427-428.

5. See, e.g., Robin M. Coupland, “Incapacitating chemical weapons: a year after the Moscow theatre siege”, *The Lancet*, Vol. 362, Issue 9393, 25 October 2003, p. 1346; and David P. Fidler, “The meaning of Moscow: ‘Non-lethal’ weapons and international law in the early 21st century”, *International Review of the Red Cross*, Vol. 87, No. 859 (September 2005), pp. 532-534.

6. Nick Lewer and Neil Davison, “Non-lethal technologies – an overview”, *Disarmament Forum*, Issue 1, 2005, p. 45.

7. See Steven Rose, “Risks”, Chapter 3.2, in *Brain Waves Module 1: Neuroscience, society and policy*, The Royal Society, January 2011, p. 76.

5. The use of explosive weapons in populated areas

There is increasing concern about the impact on civilians from the use of explosive weapons in populated areas. Drones are a concern precisely when and because they typically carry explosive weapons into an urban setting where disproportionate harm can be caused even when a legitimate military objective is being targeted in the context of an armed conflict.

And use has clearly been made in law enforcement settings, even, as in Libya and more recently in Syria, to suppress the right to freedom of expression. It is time that the use of these weapons was outlawed outside of an armed conflict as a first step to addressing the excessive harm that is too often caused to civilians.

Satellite technology and humanitarian law

Joshua Cowan Lyons

Analyst, UNITAR Operational Satellite Applications Programme (UNOSAT), Geneva

I have been a little creative in the re-interpretation of the subject matter regarding the use of geospatial technology very broadly with the United Nations (UN) – not as it relates to international humanitarian law (IHL) *per se* but as it relates to investigations of potential violations of IHL and human rights law within the UN. I have just two preface remarks regarding the content: first, if you hear me reference the “new” geospatial technologies I just want to give due respect and to clarify it. A significant majority of the technologies newly available to the UN and to the civilian community regarding satellites, geospatial analysis, GPS equipment and the like is, in fact, not new in the sense that it has been developed by intelligence and military agencies over the course of decades. So, in that respect, it is not new but it is new in the sense that it has become newly available to a community of users within the UN and the IHL community, and that we have been able to basically turn the technology on its head and use it for different purposes in a different context.

The second preface is that, for this short presentation, I will be focusing on the role of this technology as it relates to the identification and discovery of potential war crimes in two particular investigations – not as it relates to the tantalizing possibility that geospatial technology and specifically remotely sensed monitoring would act as a *deterrent* for severe war crimes or crimes against humanity. You may have heard a lot of talk recently related to the referendum in South Sudan. There’s a lot of hype that goes into this prevention issue. I have significant doubts, which I won’t address here but it may certainly come up in the conversation after.

UNOSAT is a program within the UN Institute for Research and Training (UNITAR). We have three particular core competencies. The first one concerns humanitarian aid, relief and co-ordination, that we do with situational maps as we are doing right now for the Horn of Africa crisis

– mapping IDP concentrations and movement within Mogadishu; secondly, we are now increasingly focused on human security and armed conflict and then finally a focus on territorial planning and monitoring.

Just to give you a brief overview if you are not familiar with it in the UN context. 2000 was really the watershed year in terms of our work with this technology. We had the declassification of very high resolution satellite sensors, the commercialization of what was once the exclusive domain of intelligence departments, as well as the removal of the “selective availability” program which was the deliberate scrambling of the quality of the GPS signal by the US Defense Department which meant that once this was turned off it immediately and dramatically improved the accuracy of ordinary civilian GPS devices and the technology made much more valuable for use in a humanitarian context.

Since 2000 with these two watershed events we’ve seen a very rapid adoption of geospatial technologies within the UN system for an increasingly wide range of humanitarian applications. Clearly, because of the initial stigma that was attached to the intelligence and defense world, there was a significant reluctance earlier in the 2000s for humanitarians to adopt this technology only under very controlled circumstances strictly defined as natural disasters in contexts where it wouldn’t cause any offence and it wouldn’t raise any immediate alarms. But within the last five years what we have witnessed is this initial restraint being relaxed to include the application of the same technology for explicit investigations into armed conflicts, into internal conflicts and for the investigation of IHL and war crimes and human rights violations.

Part of this is driven, I think, by the “Google Earth effect” where everyone is engaging with this technology in a personal sense, which has helped to remove this stigma and normalize it as a technology, especially for humanitarians who were once phobic about it, who didn’t even want to look at a map that had a satellite image in the background. It is important to remember that recently there were international agencies that would prohibit the use of GPS in the field for fear that it would compromise their neutrality and would be seen as combatants.

This has dramatically changed over the course of the last few years and I think that it has completely opened up the door for an increasingly more aggressive and expanding application field for this technology. This shift is reflected in our work – most of this has been published and is freely available on line. We now have many case examples that cover the conflict spectrum, ranging from traditional intra-state conflicts all the way to internal state repression, civil conflict and state neglect.

I would like to highlight two particular applications where we have used this technology recently, first being the Gaza conflict and the contribution to the Goldstone report and, most recently, our contribution to the Secretary-General's Panel of Experts on Sri Lanka report that was just released earlier this year.

Regarding Gaza and the Goldstone report, we were requested to provide geospatial support specifically in relationship to a range of particular events and questions that had been reported as allegations on the ground – and I think the prime driver for this was a justified perception that satellite-based findings in relationship to technical questions would be a more independent and objective basis to evaluate some of these competing allegations and claims, many of which seem to contradict each other. And most interestingly, I think, from a human rights investigation standpoint, it also helps to verify or challenge the voracity of particular, personal testimonies. This is always one of the open ended and weak points of an investigation when you are entirely dependent on the first hand testimony of people who are obviously affected by this event and who may or may not have some particular agenda which may influence their testimony.

To give you an overview of some of the product examples, this was a comprehensive post-conflict assessment for the whole of the Gaza Strip summarizing the analytical information that we had derived during the course of the conflict, regarding the number and type of targets as well as the incident date period. One of the illustrations from the annex of the Goldstone report was the particular targeting changes of the IAF (Israeli Air Force) along the border with Egypt – there were two critical zones illustrating a significant tightening and change in the building targeting during the last week. An important finding as illustrated in the report with this graphic was that 70% of the buildings identified as destroyed in air strikes occurred during the last week of the conflict, and this was one of the factors which influenced the Goldstone opinion in that this final round of building destruction likely constituted a breach of the Geneva Conventions.

Then, an under-reported but fascinating event that I want to highlight quickly – this is actually a detailed map, an analysis of the destruction of a sewage treatment plant in central Gaza. The image in the upper left hand corner is a high resolution image of the sewage treatment plant after it had been damaged – there's a little point marking a 22 meter crater where either an air strike or an explosive event on the ground caused a breach in the retaining wall which resulted in a literal sewage tsunami that burst forth from this treatment plant and as you can see highlighted in the orange and yellow it flowed 1.2 km in what we assume to be an extremely violent and rapid event covering over 5 hectares of land. This had not been reported at the time. The initial assumption was that this must have

been caused by an Israeli air strike and it was a consideration within the Goldstone investigation. However, if I remember rightly, they did not make any attribution for this precisely because it was impossible to really say – there was no evidence on the ground that suggested an air strike and actually the Israeli Air Force then released their own investigation of which I can think was convincingly argued that this had not been a IAF *sortie* but had in fact been a deliberate act by Hamas to cause a delay for the IDF tanks that were moving in this region. And this, in fact, is similar to what we have also seen in Sri Lanka when the LTTE, the Tamil Tigers, deliberately demolished several dams flooding vast areas of land in order to delay the troops of the Sri Lankan Armed Forces.

Just one more note. You can see on the map that there are actually ground photographs related to the analysis – these were GPS tagged photos that were taken during a UNEP field assessment – and we were able to ingest this ground data to evaluate the accuracy of the initial assessment. This is a trend that is increasingly significant when we start to imagine the potential of crowd sourced geo-tagged information that is then ingested and then combined dynamically and sometimes in real time with the satellite imagery for further analysis.

Regarding the Secretary-General's Panel of Experts' report on Sri Lanka, we received a request to provide geospatial support in the form of direct briefings to the panel as well as the provision of a substantial report – a significant percentage of that report was then included in their final report released earlier this year.

Now, I just wanted to highlight the main findings of this geospatial analysis, the satellite derived analysis, which included compelling evidence on the indiscriminate and disproportionate government shelling of no-fire zones as well as the use of civilians as human shields by LTTE forces.

To briefly show you some of the methodology in the workflow – we had been given a list of protected sites that became targets – hospitals, a UN compound, religious facilities, cultural facilities, and then we proceeded to do a detailed analysis of the impacts of the damages. The problem with this scale of analysis is precisely that most of these damages are caused by small mortars and once you are investigating this allegation: the hospital has been shelled and there is a mortar and you have witnesses it's virtually impossible to make any genuine attribution. It could have easily come from LTTE or government forces and I think this is one of the weaknesses of this traditional approach at this particular scale. So, instead what we did was we zoomed out so to speak and looked at the broader context in which these damages were occurring and what we saw clearly was that they were not in fact accidental or random or limited shelling events but they

were in fact part of a consistent and coherent, very structured campaign of indiscriminate area bombardment.

In this particular area of the second no-fire zone in Mulliativu, the different colored dots represent individual impact zones – mortar craters or destroyed buildings. Scattered amongst all of these were literally tens and thousands of civilians who were sheltering in their makeshift bomb shelters, little trenches they would dig and then dump their families into. Zooming in and looking at it between 19th April to 10th May – this is a beach zone – you can see little tiny white squares are the IDP shelters – they were pushed into the beach zone. And then we have a table summarizing the number and the final impacts. They were clearly visible on the beach zone that these shells were coming both from the water as well as from land. The analysis included air strike locations and some very basic analysis regarding the timing as well as the targets.

We should say that the conclusions were that almost all the prominent air strikes we had identified were most likely against legitimate LTTE targets, that there was clear evidence of military activity in that area at that time. Some of these, however, were clearly directed against locations likely military but nevertheless within the clearly defined government no-fire zones.

For the artillery analysis this formed the basis for most of the primary conclusions regarding the indiscriminate and disproportionate shelling – the area bombardment allegations. We were confident to be able to say that, from an operational standpoint the Sri Lankan Armed Forces (SLA) maintained an updated military capability to fire artillery – howitzers – into areas heavily populated with IDPs and specifically into the no-fire zones. Mind you, this is exactly where the LTTE had concentrated their forces. So, it is one and the same. Of particular interest we saw the SLA were deliberately rotating their fire-bearing of the howitzers as the active combat zone changed, and basically the orientation was dynamic and it followed both the movement of the LTTE and the IDPs. So, at any given moment the LTTE moved the 150 thousand plus IDPs moving along with them in exactly the same direction at the same time. Further, these sites identified as probable indiscriminate area bombardment closely match the identified artillery battery fire-bearings as illustrated here. This is an overview map of the entire conflict for the last 4 months showing the main artillery sights, attributed as best we could to either the SLA or LTTE forces.

One of the critical caveats we included in our report was obviously the limitations of the satellite imagery in the context of this asymmetrical phase of the civil war. Because the Tamil Tigers had lost their air force and they had lost most of their traditional, conventional forces they basically reverted to a traditional guerrilla-style campaign – the camouflage was

extremely heavy and everything was basically masked in civilian clothing. So it became nearly impossible for us to identify with any real confidence the rapidly deployed mobile mortar batteries for the Tamil Tigers for example. They would literally roll them out from underneath trees, fire off their rounds near a hospital for example, roll them back in and they're gone. So basically there is no way of identifying them with this type of approach.

In terms of artillery analysis, this is an illustration of the rotation – I know it's a little bit complex, a little bit hard to read if you are not immediately accustomed to it but there are 6 artillery howitzer pieces and their fire bearings are rotating dynamically. When we actually start to project where their fire capability was and then match that with the times series as well as with the progression of the IDPs, of which we were mapping in some detail as well as the changes in the shape and structure of the position of the no-fire zones, what we clearly see is that the targeting is falling distinctly within the clearly defined government-declared No-Fire Zone. I think there are significant legal ramifications regarding that designation as opposed to a no-fire zone that has been adopted by both sides.

Then, finally, if I have just a few more moments – in terms of attribution of potential criminal activity or war crimes by LTTE the one thing that we were confident about in terms of making specific charges or allegations, providing evidence to the Panel for their consideration, was that there was a conscious effort by LTTE to deliberately use civilians as a human shield to protect against SLA air strikes when they located their heavy vehicles. Most of these vehicle convoys were in fact, as reported and verified after, loaded with fuel, ammunitions, command control centers and these were placed in the areas of the highest civilian density – the map at the very bottom illustrates both IDP locations, tent shelter locations. The yellow represents vehicles taken by the LTTE – basically the Tamil Tigers had commandeered anything on wheels.

As we feared, the consequence of course was that at some point this huge and very densely packed concentration of vehicles laden with fuel and ammunitions exploded. We were actually able to detect and measure the exact time of the explosion based on thermal infrared satellite imagery that detected the active fires. This was an explosive event on 16th May which produced a zone of near total incineration absorbing hundreds of IDP tents as well as an unknown number of people. The Sri Lankan Armed Forces in their own report described a similar event not in reaction to this work but independently and what they said was that this, in fact, was a deliberate event by the LTTE basically as a delay tactic again to cause a final injury to the Sri Lankan Armed Forces. And I think that was a compelling reason why this event was not ascribed to the Sri Lankan Armed Forces but rather to the deliberate efforts of the Tamil Tigers in the last few days that they existed.

IV. Robots, remote-controlled and autonomous weapon systems

Ethics and artificial intelligence

Ronald Arkin

Regent's Professor, Director of the Mobile Robot Laboratory,
Associate Dean for Research & Space Planning, College of Computing,
Georgia Institute of Technology, Atlanta

Today, I am coming here with a serious message for you all, as I believe all my fellow panellists are too – by talking about the issues and the advent of a new technology which can have a profound impact on the battlefield. Yesterday, we heard about RMAA, the Revolution in Military Affairs – many considered the advent of robot systems and certainly I am one of those too. Why is the military doing this? The military is doing this for a plethora of reasons but the main reason, the mantras that you hear spoken in the halls of the Pentagon, elsewhere, through literature and most military robotics places – and I will give you a somewhat US centric perspective on this as well too – are these classic phrases: the notion of force multiplication – how can we do more with fewer soldiers? How can we make an individual war fighter operate more effectively in the battle space thus avoiding a disaster, lowering risk and a variety of other things? The notion of expanding the battle space, being able to fight over larger areas and larger regions due to persistence and other factors than otherwise has been available, the notion of allowing an individual war fighter to see further and to strike further than they would otherwise. And, of course, the traditional one, reducing friendly casualties, but little attention has been paid, historically, to the innocent in the battlefield, the non-combatants and the civilians. How will this technology impact upon them and I am counting on you, the people in this room to assist in making sure that as this technology moves forward, and it will move forward, that indeed it is used in an appropriate manner in accordance with international humanitarian law.

We talk about force-bearing platforms; you have no idea how many platforms there are out there and under development. This slide is two years old. The United States is very forthright in its ability to declare what's going on in an open society but rest assured that many, many other

nations are developing similar platforms – there are about 40 different U.S. platforms in various stages of development – you don’t have to read them, the most important thing to see there is just the sheer numbers. These are not just unmanned systems, these are force-bearing unmanned systems from a recent report from the Department of Defense. But our country is not blind to the potential dangers that this technology can unleash. What we must be aware of is that, as we move further and further towards autonomous systems, towards systems that actually have decision-making regarding targeting, verification, engaging and battle damage assessment afterwards, as that goes on, we need to make sure that it is done correctly. All weapon systems in the United States are subject, before they are introduced, to verification by legal authorities to make sure they are in compliance with the laws of war. These will be no exception, but the real question is what does it mean when we start truly engaging, in the AI sense, in the artificial intelligence sense, with these systems to take human life, not indiscriminately – that’s the important thing or else it would be a violation.

Here are some phrases from a recent report, it says: “the decision to fire will not likely be fully automated until legal rules of engagement and safety concerns have been all thoroughly examined and resolved”. This will not be a hasty decision but sometimes, again, we have to be cautious due to the pressures of conflict to move technology into the battlefield sometimes before its time. Another report from the U.S. Air Force flight plan, and notice the time frame – this goes out to 2047, the United States is planning to use this technology for a long, long time. It is one of the strategic initiatives or directives from the Secretary of Defense, I believe number 4, and we will continue to explore it into the near and considerably far-term for its uses. But these statements from this report saying: “authorizing a machine to make lethal combat decisions is contingent upon political and military leaders resolving legal and ethical questions. Ethical discussions and policy decisions must take place in the near term rather than allowing the development to take its own path apart from this critical guidance”. That’s why I’m here.

We need your help, I need your help. I’m a roboticist so I help partly to develop the technology, I’m certainly not fully responsible for it but I am partially responsible for the advent of some of the techniques that are used in these kinds of systems and to me it is important that they are used in accordance with international humanitarian law. Now make no mistake, I have utmost respect for our human war fighters in the battlefield. And further, I feel I have a responsibility to provide them with the best technology that our nation can provide, but saying that, it is

crucially important that we make sure that it also adheres to our nation's purported ideals which are a subscription to international humanitarian law (IHL).

The UN has talked about this as well. This is a report from Reuters – there's an interesting quote here – in a Report to the UN General Assembly Human Rights Committee Christof Heyns said: "Such systems raise considerable concerns that have almost been entirely unexamined by Human Rights or humanitarian actors". Let's examine these issues, and that's why we are having this discussion today. "The international community urgently needs to address the legal, political, ethical and moral implications of the development of lethal robotic technology", said Haynes, UN Special Rapporteur on Extra-judicial Executions. This is important stuff and it's near-term. And why is it important? This is happening, it has happened, it will continue to happen. The whole notion of lethal autonomy is a fact of life. We heard described in Dr. Kellenberger's talk yesterday too. Even landmines to a roboticist, in many respects, constitute a robot where there are sensing and actuation. The sensing is primitive for an anti-personnel mine, it doesn't do discrimination, hence the conventions arguing against its use, but the more sophisticated ones are capable of doing discrimination – from seismic signatures, from visual signatures, from infrared signatures which can discriminate between a school bus and a tank.

There are many other systems out there – by some definitions cruise missiles fit this category. The Phalanx System has an auto-mode operation which is put in for protection of Aegis class cruisers in the Navy – you turn it on if a target comes in with an appropriate signature, then it shoots it out of the sky. Why? Because there's no time to ask the captain whether this is a legitimate target or not. Even the patriot missile system, as I understand it, has about 10 seconds to basically allow the operator to shut it down and keep it from firing. Given that set of circumstances what are the conditions under which a patriot operator would be able to make an intelligent decision regarding whether that's a legitimate target or not?

Why is this all happening? Because of the increase in the tempo of the battlefield. From Napoleonic times to World War I to World War II to now the pace of the battlefield is ever increasing and, make no mistake, while we are fighting two wars, well, maybe one and a half now, against relatively unsophisticated opponents, if and when the next inter-state war comes about we must be aware that countermeasures of a variety of different sorts will be present which will continue to force autonomy to the so-called tip of the spear where the decision-making is made by the weapon and not by the human being, and I can elaborate more later if you like.

The notion of a human in a loop is a red herring in my estimation. A human in a loop doesn't really mean much of anything. At one level, it means there's a human making a decision regarding a particular piece of information coming in whether they will release the weapon or engage that target or not. In another it will be something at a higher level – go and take that building using whatever force is necessary. A variety of different things occur and you can see the trend in the language of the military where the Air Force now uses the phrase “*human on the loop*” and the army uses the phrase “leader in the loop” which speaks to more supervisory control.

All of these things cry out for inspection. We need to examine what this technology and how this technology will be used. And also people make mistakes too and sometimes – and I know some of my counterparts may differ- robots can do better, AI systems can do better. I could talk about why 9/11 should never have happened given intelligent technology but we trust human beings too much sometimes, and we allow them to override these particular systems. Sometimes the machines are smarter and the only way we can control this progression is through potential treaties or interventions.

Now, here are some rhetorical questions I'll ask. Should soldiers be robots? What do we do to human beings when we are training them? We train them to be obedient, we train them to follow orders, we train them in a way to comply with IHL for sure but we also train them to operate in a way which is somewhat unnatural given the human condition. So, the other question is could robots be soldiers? Could they ultimately out-perform humans from a morality perspective in a battlefield? We already have robots that are smarter. We already have robots that are faster. We also have robots that are stronger than human beings. Is it so hard to imagine, is it really hard to imagine, given the performance of humans in the battle space, the somewhat deplorable performance of humans in the battle space, that they cannot treat us better than we treat ourselves? This audience should know better than anyone else having borne witness no doubt to the atrocities worldwide that have been committed in the conduct of warfare of every nation in every conflict.

So, what role can technology play in actually reducing these kinds of infractions? The United States did a survey back in 2005 of the returning war fighters from Operation Iraqi Freedom and they inspected both their mental health and their moral performance – first time in the history of our nation and probably of any nation. The numbers are quite disconcerting. I'm not going to go over them – they are available on papers and on our website and from the report which is publically available as well too, but it

talks about 45% of soldiers and 60% of marines did not agree they would report a fellow soldier if they had injured or killed an innocent combatant. Is that not a war crime even of itself? 17% of soldiers and marines agreed or strongly agreed that all non-combatants should be treated as insurgents – they are no non-combatants in the perspective of almost one in five in the battle space. And so on and so on. These numbers are discouraging but they are not unique to the United States. This is, as you know, and I am convinced that everyone in this room knows of the problems of human beings fighting in the battle space. So, again, I ask you what can technology do?

These are the reasons why soldiers act this way – they are well documented. For roboticists like me to have to read books regarding people killing civilians was hard to wade through to be honest with you but it is crucially important that my community understands the consequences of the potential of the technology we are creating. My contention is that many of the causative problems human beings suffer from when engaged in warfare, autonomous systems do not have to suffer from.

So, this is the underlying research thesis. This is a hypothesis, this is a testable hypothesis and some of my research funded by the Army Research Office has addressed this particular issue: trying to understand if robotic systems can ultimately be more humane than human beings in military situations? We shall talk about what those military situations are and I am not talking about replacing the full moral faculties of human beings. I am talking about highly constrained, highly restricted circumstances where human soldiers often find themselves in very dangerous situations and may act in ways that veer outside the bounds of international humanitarian law. Notice also that I make no claim that these systems will be perfect. I know of nothing in this world that is perfect and these systems will fail too. The benchmark for acceptance in my estimation is when they out-perform human war fighters and if they can out-perform human war fighters not just from a mission perspective but from an ethical perspective that translates into the saving of non-combatant lives, the reduction of non-combatant casualties and the reduction of destruction of non-combatant property.

So, if we can do that, to me that is a step forward. Why do I believe this? Well, look what happened this year alone in artificial intelligence. I don't know if you have in your own country a version of "Jeopardy" but one could argue that it is the intelligentsia of game shows, where we had a computer system that competed against the very best champions this game show has ever had. It wasn't hooked up to the internet, it couldn't do queries on the internet and it beat them. In Brazil, and I don't know

how well the system works but they are trying to use this eyeglass facial recognition system to identify terrorists at the Olympics. And mostly of note is that Nevada has just recently authorized the use of autonomous systems on their highways – one of our States, thanks to Google. Google, which is assisting in building autonomous vehicles, claims that if we want to save lives we need to put robots on the road and take humans off the road. It's the humans that are the problem, not robots, and that is my claim as well to some degree in the battle space, although I don't think Google would be fully comfortable with that parallel argument.

In any case, from the research perspective, these are the things I have strived to produce in our systems to provide a robotic system the right to refuse an order that it deems unethical. That doesn't always go over so well with the military as you might imagine but nonetheless it needs to be able to explain its decisions. It also needs to potentially be able to report and monitor the behavior of others in the battlefield. It should also incorporate the existing laws of war and other protocols and rules of engagement into its actions.

Now, I do not advocate these robots as I said for one on one replacement for human soldiers, as these will work alongside human soldiers and not serve as a replacement. I also discourage their use in counter-insurgency operations such as the situations we find ourselves in right now – this refers to the lethal autonomous aspect due to the high population of civilians and the current low capability to do discrimination. Now, what needs to be done in my estimation is a graded introduction of these systems into the battle space and dealing with highly specialized missions, not unlike dogs or specialized platforms that have been used in the past for certain scenarios particularly for room clearing operations such as occurred to poor effect in Haditha, counter sniper operations, or as deployed in South Korea for perimeter protection of the de-militarized zone. I believe one of my colleagues, Noel, will be talking about this perhaps later.

Now, why do I believe this should be done or could be done? There is a variety of reasons and I do not have the time to explain them all. But I shall mention them in passing. Robots have no inherent right to self defense. They can act conservatively, so they can truly assume risk on behalf of non-combatants as opposed to telling a soldier he/she is required to assume risk on behalf of non-combatants. Well, for the human, that is easy to say but it is not so easy to do. For a robotic system it is easier to do better under these circumstances. I firmly believe, especially given the recent developments, these systems will have better sensors and better capabilities than humans will ever have under these conditions. We can engineer out the emotions of anger, fear, frustration and other things within

these systems that can potentially lead to the kinds of problems humans have. There is another psychological problem called “scenario fulfilment” – I don’t have time to talk about that but I’ll be glad to answer questions later if you like.

Further, with the advent of network-centric warfare, as we heard yesterday, the notion of their ability to integrate far more information from far more sources far faster than any human being possibly could is greater. You see human pilots turning off their heads-up displays because they can’t process all the information coming to them. In this case, these systems, could in the future – I’m not talking now, I’m talking in the future – 10 to 20 years from now if this avenue is pursued, be able to have these capabilities. And finally, they have the potential also for recording and reporting aberrations from an IHL perspective. We talked about that a little bit in the second to last talk yesterday where you can use these systems for observation, whether it’s a satellite or a UAV or a ground vehicle for being able to potentially change the behaviour of the humans in the battle space as well.

There are many, many reasons why people say this can’t be done. This is the list I’ve built over my talks in many, many different places. I think that Noel will speak about a few of them including mission Creep and proliferation. I’ve mentioned refusing an order, establishing responsibility is a crucial one – you can never ever say the robot did it. Somehow responsibility has to be attributed to human beings somewhere. We’ve handled that by the design of a responsibility advisor and the intelligent deployment and understanding of what’s required for these systems in the battle space, but somewhere a human being must be held accountable if things go wrong. There are many, many effects from a military perspective as well, the effect on squad cohesion, which means if you have a robot that will tell on you if you did something bad that destroys the so-called “band of brothers” effect. You need to be worried about that because then in Vietnam and other places they “fragged” people, so they may frag the robot or destroy the robot under those sets of circumstances. But if this robot can potentially take a bullet for you, can do better than Joe can in watching your back, can go round the corner and you don’t have to go round the corner maybe that’s an appropriate price to pay in changing your behavior accordingly and if that advances subscription to the ideals embodied in international humanitarian law that is a step forward.

In the research I conducted, and I’m not going to talk about the technical aspects of that, that’s not relevant here, there are plenty of sources for that. We embed the establishment of responsibility, military necessity, discrimination or distinction, and we looked at the principle of double intention which goes beyond the principle of double effect. Double

intention arose from the Just War theorist Michael Walzer as a means for deliberately reducing civilian casualties rather than merely tolerating it. By computing proportionality, conceivably using faster than real time simulations, and using battle damage effects rather than seat-of-the-pants calculations or experiential calculations that fighter pilots or others may do before engaging or allowing the engagement of the target, we may be able to outperform humans in this respect.

These are some of the components, some of the aspects, and most of these are incorporated in the “Ethical Governor”, which deals with a bolt-on component which allows lethality to occur or not; also the ethical adaptor that actually embodies an analogue of a moral emotion called guilt. I could describe some of the aspects used with that, that have been shown by Generals such as McChrystal in the restriction of weapon systems in their use when their effects are not well understood and how that can be embedded within the system as well too. And the notion of the responsibility advisor. This has been tested in a variety of simulated scenarios – I do not have any lethal robots in my laboratory and I don’t want any lethal robots in my laboratory – some of the scenarios are cases often based on real world events where requests had to go all the way up to the Pentagon to determine whether a system would be allowed to fire. In one case, firing was denied under this particular set of circumstances due to the rules of engagement but it’s a no-brainer for a UAV to use GPS and “no-kill” zones or outside of “kill-zones” in this one particular case to make this decision without bothering the JAGs out there who have to make a recommendation.

There is another scenario based on human performance, a video that most military in the United States have seen at one time or another, which deals with questionable behavior by human soldiers with someone who is apparently, and I am not a lawyer, *hors de combat* at the end and that individual to use the military phrase, was neutralized from a stand-off weapon system. The analogue of going up and putting a gun to that individual’s head is comparable. I don’t know if you saw the video from Syria just the other day where they were pumping bullets into a near dead individual purported to be from the Syrian ground forces. The Korean DMZ (de-militarized zones) platforms are being deployed, given the heightened tensions that occurred after a recent incident on that island attacked by North Korea, and finally an urban counter-sniper scenario is the one we would like to test down at Fort Benning if we follow on this work.

If you are interested in seeing these things in simulated operation just visit my website or send me an e-mail. There are narrated scenarios which describe the operation of these particular systems.

So, in conclusion, I can say that this is not a done deal, this is an approach. We have taken baby steps towards the accomplishment of this idea. The work I did was what I refer to as proof of concept, something can be done, in very narrow restrictions where bounded morality applies, where you do not have to embody the entire laws of war and rules of engagement but you narrow them down to very mission-specific, content-sensitive circumstances. But even then, there are many, many daunting questions remaining. To accomplish this requires the standing up of a large research community and I have been in discussions with some of our folks about potentially having that occur. Whether it does or not I don't know but I've given it my best. My community as well, as a bunch of roboticists, is largely ignorant, and to be self-critical as I was too, of the consequences of the work we are doing. Most of the time we just started trying to get something to go from point A to point B and now we're trying to get it to go from point A to point B with a gun on it. And if there is good work by our community someone, somewhere, sometime, someplace will embed that in a military system. Folks like Bill Joy in his article "Why the future doesn't need us" argues for complete relinquishment of robotics research as it will lead to the extinction of mankind – that is a bit extreme – but nonetheless, I think we need to be wary about how we proceed and we need to be proactive about this. As I also mentioned we already have a prototype proof of concept architecture and I hope to test this in other domains too.

Operational advantages and risks in the use of UAVs

Eugene Miasnikov

Senior Research Scientist, Center for Arms Control,
Energy and Environmental Studies, Moscow

It is quite a challenge to speak to this audience as many of you have substantial expertise in the problem I am going to talk about. Nevertheless, let me try to identify the key issues from a prospective of a Russian analyst with a technical background. I hope to be able to help in stimulating a constructive discussion on these issues.

Perhaps, it is more appropriate to talk about unmanned aerial systems rather than vehicles, as we consider operational advantages of UAVs (unmanned aerial vehicles). What makes potential customers interested in using UAVs? The fact that a UAV is operated as an element of a system which includes an infrastructure on the ground, reliable communication and information distribution links, so that the customer gets the final product in a usable form and in a timely manner. Otherwise, UAVs remain promising experimental tools showing some potential, but not ready yet to be used on a regular basis.

Many countries are currently producing UAVs, but only few of them as the United States or Israel passed the gap of creating such a system. A notable example is Russia with its strong aviation industry. Over a dozen Russian companies are currently offering experimental UAVs, but potential customers like the Russian Ministry of Defence, the Ministry for Internal Affairs and the Ministry for Civil Defence and Emergencies are buying these UAVs in very limited numbers mostly with a purpose to assess their potential. Apparently there is a demand there, but thus far there is also a lack of unmanned system technology solutions.

What operational advantages can unmanned systems offer? The answer is well known. They can perform the tasks that are dangerous, dull or “dirty” for piloted airplanes, like intelligence, surveillance and reconnaissance (ISR) operations or various combat missions. They can also offer more affordable solutions in civilian applications, compared to those

that are currently implemented. This list can be continued. Perhaps, it does not make sense to spend more time discussing operational advantages. You may find them in every commercial booklet on UAVs.

What about the risks?

The focus of our meeting is to discuss risks occurring because a practice of unmanned system application creates contradictions with International Humanitarian Law (or it may create in future). Practices, such as CIA drone operations in Pakistan and other places raise good and timely questions. In particular:

- What is the legal basis for this kind of operations?
- In which circumstances can an operator of a remotely piloted vehicle decide to use lethal weapons against suspects?
- Who is to blame for a collateral damage, for deaths of civilians and especially of children that result in such operations?

There is also a big question for the future (which was the focus of Prof. Arkin's talk): will humankind be able to delegate the right of making decisions to robots on a use of lethal weapons? The answers are needed fairly soon as technology apparently is moving fast in this direction.

The problem of using weaponized drones (UCAVs/Unmanned Combat Aerial Vehicle) is, of course, much broader. Some analysts put it this way: Does the practice of targeted killing with the use of drones really solve the proclaimed goals, make the region a safer place and contribute to sustainable development? If the answer is "No", we have the risks of further destabilization of a political situation in the regions with a huge impact on the rest of the world.

Contradictions with the existing legal norms are not necessarily limited to military systems. In particular, one may raise the question as to how the basic human right to have a private life can be protected, as UAVs are increasingly used for surveillance purposes by police or security forces. Who is to decide whether such methods of gathering evidence are legal and under what circumstances that is the case?

There are also risks of a different nature. At a first glance they are beyond the scope of our Round Table. However, I'd suggest that we consider them here. Risks of a different nature require differing solutions. Let me make a point, that seeking those solutions may create some synergies and help to solve the problem we are primarily focused on.

What are those other risks I have in mind?

1. The risks associated with the fact that most unmanned systems are not sufficiently reliable yet by existing common technical standards. Frequently UAVs malfunction or go out of control, which may result in significant costs. UAVs are not cheap by themselves. UAVs may also cause

significant damage as they fall on the ground in urban areas. Finally they share airspace with manned aircraft. Fortunately, the pilots of U.S. Air Force C-130 airplanes managed successfully to land after a mid-air collision with RQ-7 Shadow UAV in the skies of Afghanistan this August, but, as you can imagine, it could have been much worse.

2. The risks occurring by assigning UAVs military roles (especially offensive ones) by one state, may cause legitimate concerns and reaction by other states, and stimulate regional arms race. In my opinion, it is extremely important to be aware of these risks as humankind pursues the goal to get rid of the most dangerous and devastating tools of war – weapons of mass destruction.

In particular, efforts to get rid of nuclear weapons may be undermined by current trends in development of conventional arms, especially in the United States. In particular, one of the directions of unmanned aerial system evolution as Dr. Neuneck and Dr. Hitchens told us yesterday is developing hypersonic long-range unmanned combat aerial vehicles for accomplishing Prompt Global Strike missions. Let me remind you, that the Prompt Global Strike program currently aims at developing a capability to deliver a limited conventional kinetic strike anywhere on the globe within half-an-hour – one hour timeframe. By the way, systems, developed for ISR purposes, may also have a role in the Prompt Global Strike missions, as there is a need for guidance of the strikes and post-strike damage assessment. Another direction of UAV evolution – is their potential use in ballistic missile defence systems, particularly those that are intended for boost-phase intercepting.

Development of unmanned systems in the US is watched attentively in Russia. There is a common view shared by the majority of Russian analysts, that the next phase of nuclear reductions will require setting limits on strategic conventional arms. Ballistic or hypersonic missiles armed with conventional warheads are considered as destabilizing arms, since they might have the capability to disable strategic ICBM launchers. It is interesting, that when New START Treaty was discussed by Russian legislators in the State Duma in January this year, the draft law of the Treaty ratification, proposed by the Communist faction, contained a requirement that prior to the ratification Russia and the US should conclude treaties limiting UAVs among other things. This draft was rejected. However, I'll not be surprised, if the issue is raised again in the near future.

3. Finally, there is also another group of risks. As the UA systems are developed, we need to ask a question: what might happen if they turn out to be in the wrong hands of non-state actors, like terrorists? This

issue has been studied in our Center. The results of the study were published seven years ago in a report that can be accessed at our Center's website www.armscontrol.ru.

Let me just very briefly summarize the conclusions of the study.

The threat of terrorist UAVs is not the top item in the threat priority list these days. Nevertheless, it exists and it will eventually grow as UAVs more and more enter into our life.

Even small payloads of a few kilograms can create significant damage and mass casualties, especially in the case of biological or chemical weapons.

The most likely threat may occur from mini-UAVs. The most worrisome situation stems from model aircraft, where uncontrolled access to the knowledge, skills, and equipment required for mini-UAV assembly exists.

The main accent when dealing with the threat of terrorist UAVs needs to be on proactive measures. I believe the key to the answer is educating the culture. There is a role here for governmental agencies and NGOs. There is little chance to stop a terrorist UAV attack, unless the general public is made aware of the threat and its potential consequences.

Drones proliferation and protection of civilians

Noel Sharkey

Professor of Artificial Intelligence and Robotics, University of Sheffield

The recent Iraq, Afghanistan and Gaza conflicts have created a dramatic increase in the use of remotely-piloted armed drones. With over 50 countries now buying and developing the technology, autonomous armed drones could become dominant in future war. Although there is currently a “man-in-the-loop” for all lethal targeting operations, that role is set to shrink rapidly as more autonomous operation becomes available. Current autonomous robots cannot discriminate between combatant and non-combatant targets, do not have battlefield awareness, cannot reason appropriately or make proportionality decisions. We point to the dangers of relying on future technological fixes and examine the impact on International Humanitarian Law. Military necessity is considered as a possible way to allow new indiscriminate weapons to be deployed.

1. Proliferation

In the post-9/11 era, aerial drones have come to dominate military operations. Troop movements are almost always accompanied by intelligence, surveillance and reconnaissance drones. The military success of UAVs (Unmanned Aerial Vehicles) in the theatre of war in Iraq and Afghanistan has created massive worldwide demand for the technology. It is massive business. The Teal Group has estimated that the market will increase to \$11.3 billion per year over the next decade, not including the billions of dollars in development costs. Teal does not have access to the figures for military robotics spending from major countries such as Russia, China or Iran¹.

1. Teal Group Corporation website, <http://bit.ly/psA7rB> (accessed 1 September 2011).

There are now at least 50 countries using UAVs². Many of these are being developed in-house and many are being bought in (and probably copied). The US sells many of its drones to its closest allies in Europe and recently the US Company General Atomics has been given permission to sell its earlier generation predators in the Middle East and Latin America. Israel has an even wider range of markets, having recently expanded into Latin American countries. Countries that do not have the advantage of being a close ally of the US cannot yet buy armed drones, and so they are having to find other means of acquiring or developing them. India and Pakistan are working hard to develop attack drones, having failed to purchase any from the US or Israel. Russia has shown models of the MiG Skat unmanned combat aircraft, which is intended to carry out strike missions on air defences. It is, according to reports from Russia, able to carry cruise missiles and can strike both ground and naval targets. Iran demonstrated a rocket launched UAV, the Karrar or ambassador of death, to the press in 2010. It carries two cruise missiles. It is not possible to ascertain how operational the Iranian and Russian craft are, but it is clear that, at the very least, they are moving in the right direction to make the technology.

China is showing the greatest commercial potential for selling armed UAVs over the coming decade. It has made a showing of many different types of UAV at its air shows over the last five years, some almost replicas of the US drones. The US-China Economic and Security Review Commission said that China “has deployed several types of unmanned aerial vehicles for both reconnaissance and combat”³. According to the *Washington Post*, at the Zhuhai air show in China in November 2010, there were more than two dozen Chinese UAV models on display⁴. Worryingly, the *Washington Post* quotes Zhang Qiaoliang of the Chengdu Aircraft Design and Research Institute as saying, “The United States doesn’t export many attack drones, so we’re taking advantage of that hole in the market”.

2. I have personally read valid robotics reports for each of the following countries, and there may be many more: Australia, Austria, Brazil, Bulgaria, Canada, Chile, China, Columbia, Croatia, Czech Republic, Ecuador, Finland, France, Germany, Greece, Hungary, India, Indonesia, Iran, Israel, Italy, Japan, Jordan, Lebanon, Malaysia, Mexico, Netherlands, New Zealand, Norway, Pakistan, Peru, Philippines, Poland, Romania, Russia, Serbia, Singapore, South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan, Thailand, Tunisia, Turkey, United Arab Emirates, United Kingdom, United States of America, Vietnam.

3. 2010 Report to Congress of the US-China Economic and Security Review Commission, November 2010, p. 79 available via www.uscc.gov.

4. William Wan and Peter Finn, “Global Race On to Match us Drone Capabilities”, *Washington Post*, 4 July 2011, <http://wapo.st/mfRa62> (accessed 10 August 2011).

This is worrying because it indicates the opening up of a large and expanding market of which all the major players will want a share. If it looks like China's combat UAVs threaten to dominate the market, then others will start selling them and every developed nation will have them. This could have a significant impact on how disputes are handled and what constitutes a war.

2. Autonomy and the pace of battle

Since 2004, all roadmaps of the US forces have made clear the desire and intention to develop and use autonomous battlefield robots. Execution of these plans to take the human out of the loop is well underway. The end goal is that robots will operate autonomously to locate their own targets and destroy them without human intervention⁵.

Autonomous lethal targeting is not illegal so long as it accords with the principles of distinction and proportionality. In a military rich environment with few civilians in, say, a desert or at sea, there may be a few problems with using armed robots to kill targets. Legally, this may be little different from firing rockets from a distance, dropping bombs or sending cruise missiles. However, armed robots are set to change the pace of battle dramatically in the coming decade. It may not be militarily advantageous to keep a human in control of targeting.

The speed of an unmanned craft is limited only by the integrity of its structure and components and not by human G-force limitations. Unmanned planes cannot only travel faster than piloted planes but can also manoeuvre much faster, taking sharp turns that would kill a human pilot.

The US has been testing the supersonic Phantom Ray and the X-47b. The US Navy would like to replace the F-35s on their carriers with the X-47b⁶. The Chinese (Shenyang Aircraft Company) are working on the Anjian (Dark Sword) supersonic unmanned fighter aircraft, the first UCAV designed for aerial dogfights. DARPA (Defense Advanced Research Projects Agency) and the Pentagon want armed unmanned vehicles that can reach anywhere on the planet within 60 minutes. The DARPA HTV-2 program is a good example of the direction of technological developments. The Falcon

5. Noel Sharkey, "Cassandra or the False Prophet of Doom: AI Robots and War" (2008) 23(4) *IEEE Intelligent Systems* 14.

6. "USN Wants to Replace F-35s with UAVs", *Strategy Page* (online), 11 September 2011, www.strategypage.com/htm/htnavai/articles/20110911.aspx (accessed 11 September 2011).

HTV-2 is a hypersonic unmanned plane that in recent tests flew at a velocity of between 17 and 22 Mach, i.e., 17 to 22 times the speed of sound at its altitude. That is a maximum speed of 13,000 mph (20,921.5 kph), which is around 8.5 times faster than the Russian MiG-25, maximum velocity Mach 2.3 (1,520 mph or 2,446 kph).

However, as with any mobile system controlled by complex software we cannot predict how it will react in all circumstances. A series of unpredictable events could occur, or there could be an undetected bug in the program or a hardware fault. A hypersonic drone could be off target by 5 km in less than a second.

A simple example of just two interacting software algorithms running out of control happened on the Amazon website. The out-of-print 1992 book *Making of a Fly* usually sells for around \$50. But on 19 April 2011 Borderbooks were selling it for \$23,698,655.93 (plus \$3.99 shipping) on the Amazon website⁷. This astonishing price was created because an automatic algorithm from bookseller Profnath was interacting with Borderbooks' automatic algorithm. The story is that when Borderbooks does not have a book in stock, they automatically list it at 1.27059 times the price of the highest other seller. So, when a customer orders it from them, they can buy and sell at a profit. The problem was that Profnath's algorithm made their prices 0.9983 times the highest price of other booksellers. So, each time Borderbooks increased their price so did Profnath and they spiralled out of control.

This was quite harmless, as no one was prepared to pay these kinds of prices. However, imagine two or more complex algorithms interacting on high-speed armed robots. Without any knowledge of the other algorithms, there is no way to tell what would happen. They might just crash into one another or into the ground, or they might end up unleashing their destructive power in completely the wrong place. The point is that software algorithms on autonomous armed drones spiralling out of control is something to be very seriously concerned about.

As I have written elsewhere⁸, allowing robots to make decisions about the use of lethal force could breach both the principle of distinction and the principle of proportionality as specified by international humanitarian law. These are the pillars of the laws of war. Currently and for the foreseeable

7. Mike Eisen, "Amazon's \$23,698,93 book about flies" (it is NOT junk, 22 April 2011), www.michaeleisen.org/blog/?p=358 (accessed 10 September 2011).

8. E.g. Sharkey (no. 14); Noel Sharkey, "Grounds for Discrimination: Autonomous Robot Weapons" (2008) 11(2) *RUSI Defence Systems* 86; Noel Sharkey, "Saying No! to Lethal Autonomous Targeting" (2010) 9(4) *Journal of Military Ethics* 299.

future no autonomous robots or artificial intelligence systems have the necessary properties to enable discrimination between combatants and civilians or to make proportionality decisions.

Under the principle of distinction, only combatants/warriors are legitimate targets of attack. All others, including children, civilians, service workers and retirees, should be immune from attack. The same immunity covers combatants who are *hors de combat* – those who are wounded have surrendered or are mentally ill⁹. The principle of proportionality applies in circumstances where it is not possible to fully protect non-combatants in an action. It requires that the loss of life and damage to property incidental to attacks must not be excessive in relation to the concrete and direct military advantage anticipated.

Distinguishing between civilians and combatants is problematic for any robot or computer system. First, there is the problem in the specification of “civilian-ness”. A computer can compute any given procedure that can be written as a programme. We could, for example, give the computer or a robot an instruction such as, “if civilian, do not shoot”. This would be fine if and only if there was some way to give the computer a precise specification of what a civilian is. The laws of war don’t help. The 1949 Geneva Convention requires the use of common sense to determine the difference between a civilian and combatant, while the 1977 Protocol essentially defines a civilian in the negative sense as someone who is not a combatant.

Two major software components are necessary for robots to distinguish between combatants and non-combatants. The first is highly accurate and discriminative sensing and vision systems. While technology has improved dramatically over the past 50 years, the development of software for vision systems has been very slow. Currently, we have vision systems that can detect whether something is a human or not by its shape, although these can easily be fooled by a mannequin or a dancing bear. We have faced recognition systems that are effective so long as individuals stay still long enough to be identified, and we have various biometric tests for people who are stopped. In the fog of war all of these methods would run into insurmountable difficulties.

The second necessary component is reasoning from situational awareness. It is unclear as to when we might even get a foot in the door for this problem. There are always optimists, but the truth is that such systems are in the realm of ‘hope ware’ rather than software. There is no way to be

9. But see also John S. Ford, “The Morality of Obliteration Bombing” (1944), 5, *Theological Studies*, 261.

certain that they will never be achieved, but equally there is currently no evidence to suggest that they will ever be achieved. If they are achieved, it could be in hundreds of years.

In terms of the laws of war, we must go on the information and evidence that we currently have. We should not rely on technological fixes that are just around the very elastic corner that we may never reach. The bottom line is that autonomous robots that can kill without a human making the lethality decisions are indiscriminate weapons. They may properly belong in the United Nations Convention on Certain Conventional Weapons (ccw or ccwc)¹⁰.

3. Military necessity

The statement ‘Armed robots will always have a person somewhere in the loop for lethal targeting decisions’ is often repeated by Western powers. But saying ‘somewhere in the loop’ is not the same as saying that a human will always make the lethal targeting decisions. There are clearly instances where military necessity may override having anyone in the loop. In the extreme, if the very survival of the State was at stake and it was possible to use autonomous armed robots to save the day, it is fair to say that they would be used.

In these circumstances the use of autonomous killing machines may even be considered a legitimate action – or, at least, such an action might not be considered to be illegitimate if judged relative to the International Court of Justice’s decision, or more properly non-decision, regarding the use of nuclear weapons by States. As is well known, 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)¹¹. It would not be too fantastic to imagine the phrase ‘autonomous armed robots’ being substituted for ‘nuclear weapons’. Armed robots are a lesser beast than nuclear weapons – unless they are armed with nuclear weapons of course. So, the substitution is easy. However, it is likely that it would take much less than the imminent

10. 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.

11. ICJ, *Legality of the Threat or Use of Nuclear Weapons* (General List No. 95) (8 July 1996).

collapse of a State before indiscriminate autonomous robots were deployed.

History is littered with many examples in which humanitarian considerations have been overridden for the protection of soldiers rather than for the survival of the State from imminent collapse.

The attacks on the French market town of St. Lô during the Normandy invasion by allied forces in 1944 provide a good example of the indiscriminate use of air power. Although the town was full of friendly French civilians, an elite German Panzer division residing there was blocking the allied forces from breaking out of Normandy. Canadian, US and British forces took very heavy casualties. In response, according to Cohen, “The town was attacked on 25 July, by 1,500 heavy bombers, 380 medium bombers and 550 fighter bombers, one of the largest air attacks in World War II. Panzer Lehr was virtually wiped out, and the town was turned into rubble”¹². The path was cleared for the allied advance, but many thousands of French citizens lost their lives in the process.

These actions were (and are still being) defended on the grounds that they were necessary to achieve military success. It is argued that the bombings were directly proportional to the military advantage gained. On the other hand, Walzer has robustly argued against the actions on moral grounds and in terms of just war¹³.

Another case of ‘military necessity’ was the practice of US troops in Korea and Vietnam of firing back at targets in areas laden with civilians when they came under enemy fire. When the troops were pinned down they automatically employed tanks to return fire into hillsides as well as call for air strikes and artillery support. These actions, whilst saving the lives of US troops, indiscriminately killed civilian men, women and children¹⁴.

Cohen points out that this was not an illegal act. The law of war is not necessarily moral; it “allows troops under fire to fire back without ascertaining that there are no civilians mingled with the troops who are firing upon them. It allows troops under fire to fire back even if they know civilians are mingled with the enemy”¹⁵. Does this mean that if soldiers are fired on, then lethally autonomous robots could be deployed in the same way as artillery or indiscriminate air strikes?

If countries at war or in conflict have armed autonomous robots that will save many of their soldiers’ lives, will the deployment of those robots

12. Sheldon M. Cohen, *Arms and Judgment: Law, Morality, and the Conduct of War in the Twentieth Century* (Westview, 1989), 34.

13. Michael Walzer, *Just and Unjust Wars* (Basic Books, 2006).

14. *Ibid.*

15. Cohen (no. 22).

be deemed a military necessity? If it impacts both on the protection of soldiers' lives and on the ultimate success of the mission, then there will be a great temptation to use the technology. Imagine a situation where UAV deployment is what is giving State A the edge in an armed conflict with State B. Now imagine that State A has its communications disabled and its radio and GPS signals jammed. If State A can return to its advantageous position using its stock of (indiscriminate) autonomous armed UAVs to maintain its advantage, will it not do so?

Pushing the point home further, suppose that, having disrupted the remote control of State A's UAVs, State B now deploys autonomous attack craft; will State A not follow suit? Will concerns about keeping a person in the loop or unleashing possibly indiscriminate weapons prevent the use of lethal autonomous UAVs? It seems unlikely that a country will lose a war because it decides that moral superiority is more important than victory.

4. Actions short of warfare?

We can gain insight into the likely future use of armed drones when every major power is regularly deploying them by looking at some of the legal and political loopholes already being created in US. We start with the recent argument between President Obama and the US Congress over the War Powers Resolution. The US 1973 War Powers Resolution limits the ability of a president to wage war without Congressional approval. The president is required to obtain congressional approval or terminate a mission within 60 days and did not do so for the United States' role in NATO's Libya mission.

Harold Koh, the most senior lawyer in the state department, has strongly defended the legality of US military involvement in Libya without Congressional approval. A report to the US lawmakers explaining why the President did not need to seek Congressional approval stated: "US operations do not involve sustained fighting or active exchanges of fire with hostile forces, nor do they involve the presence of US ground troops, US casualties or a serious threat thereof"¹⁶.

There are at least two important questions that need be addressed here. The first is this: are drones now considered to be action short of warfare? As

16. Letter from the President on the War Powers Resolution, 15 June 2011 www.whitehouse.gov/the-press-office/2011/06/15/letter-president-war-powers-resolution (accessed 17 August 2011).

the White House told the *New York Times*: “American involvement fell short of full-blown hostilities”¹⁷. The second question is, does the use of remotely piloted armed aircraft constitute the introduction of armed forces or not?

The use of drones by US intelligence forces for targeted killing has been carried out in at least three other countries that the US is not at war with: Somalia, Yemen and Pakistan. Although the US will neither confirm nor deny the strikes officially, the *Asia Times* has called the CIA drone strikes “the most public ‘secret’ war of modern times”¹⁸. In 2008, the former Director of the CIA, Leon Panetta, told the Pacific Council on International Policy: “it’s the only game in town in terms of confronting and trying to disrupt the al-Qaeda leadership”¹⁹. Revealing the CIA’s intentions regarding the expansion of targeted drone kills, Panetta went on to say of al-Qaeda that, “If they’re going to go to Somalia, if they’re going to go to Yemen, if they’re going to go to other countries in the Middle East, we’ve got to be there and be ready to confront them there as well. We can’t let them escape. We can’t let them find hiding places”²⁰.

This is a dangerous precedent which is, at best, legally questionable under International Humanitarian Law as pointed out by Philip Alston, UN Special Rapporteur on extrajudicial killings. He challenged the legality of the targeted killings at a UN General Assembly meeting in October 2009. There are no independent means of determining how the targeting decisions are being made. It remains unclear as to what type and level of evidence is being used to make decisions that effectively amount to death sentences by Hellfire missiles for non-state actors. The suspects are not provided with an opportunity to an appeal or even to surrender. It is also unclear as to what other methods, if any, are exhausted or attempted to bring the suspects to justice. The whole process is taking place behind a convenient cloak of national secrecy.

A subsequent report by Alston in 2010 to the UN General Assembly²¹

17. Charlie Savage and Mark Landler (2011), “White House Defends Continuing us Role in Libya Operation”, *New York Times*, 15 June 2011, www.nytimes.com/2011/06/16/us/politics/16powers.html?pagewanted=all (accessed 3 August 2011).

18. Nick Turse, “Drone Surge: Today, Tomorrow and 2047”, *Asia Times*, 26 January 2010, www.atimes.com/atimes/South_Asia/LA26Df01.html (accessed 17 July 2011).

19. Leon Panetta, *Director’s Remarks at the Pacific Council on International Policy*, Central Intelligence Agency, 18 May 2009, www.cia.gov/news-information/speeches-testimony/directors-remarks-at-pacific-council.html (accessed 23 September 2010).

20. *Ibid.*

21. Philip Alston, Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Addendum, Study on Targeted Killings* (28 May 2010), UN Doc A/HRC/14/24/Add.6.

describes drone strikes as violating international and human rights law because both require transparency as to the procedures and safeguards that are in place to ensure that killings are lawful and justified: “[A] lack of disclosure gives States a virtual and impermissible license to kill”. Some of Alston’s arguments also revolve around the notion of ‘the right to self-defence’ and whether drone strikes are legal under Article 51.

It appears that the US does not consider the CIA strikes or the deployment of armed drones in Libya as acts of war. How far will this go? All of the countries that have been subject to strikes are militarily inferior and pose little threat to western nations. It seems unlikely that more militarily sophisticated countries such as China or Russia would see such actions on their territory as actions short of war. The precedent is now in place and what happens when other countries start doing the same?

5. Conclusion

After nearly a century of development, the Unmanned Aerial Vehicle has become perhaps the most desired asset amongst the modern militaries of the world. The military successes of UAVs in post-9/11 conflicts have created a rapid proliferation of the technology. Although there is currently a ‘man-in-the-loop’ for lethal targeting operations, that role will shrink incrementally until there is a capability for fully autonomous operation. The autonomous functions are likely to be ready long before robots will be able to distinguish between combatants and non-combatants in any way that requires battlefield awareness. They will not be able to reason appropriately or to make proportionality decisions barring some incredible and unpredictable technological breakthrough.

Concerns over the proliferation of the technology were expressed in this paper. The United States and Israel are currently well ahead of the field in terms of armed robot planes, but that may change in the near future. Russia has plans for armed unmanned combat aircraft, Iran claims to have them, and China is catching up quickly. More than 50 countries have been buying and developing the technology. It was pointed out that China will soon start selling and exporting its armed drones on the international market.

If they are not stopped, autonomous drones will likely be the tool of choice in future wars. While there is a lot of talk that humans will remain in the loop to make lethal targeting decisions until the robots can be shown to be capable of obeying the principle of distinction, it is likely that military necessity will dictate that this constraint is dropped whether the

robots are fully compliant with international humanitarian law or not. The mantra could then change to “Don’t worry, there will be technological fixes in the future”. This is similar to what the US has said about not signing the treaty banning cluster munitions.

The eventual proliferation of autonomous armed robots raises many questions of concern. What will happen when two complex algorithms meet in battle? Will the use of drones lead to lowering the bar to war because they appear to make it ‘risk free’? Early indications from the current US administration are that drone use is already being considered an action short of warfare. What dangerous precedents are being set up by the current spate of CIA decapitations for when other countries have similar technology?

It is unclear what changes will need to be made to current international humanitarian law. International humanitarian law clearly covers the requirements for discrimination and proportionality. However, the mapping between the new technologies and international humanitarian law can be problematic when the operational detail of the new technology is not clear and keeps changing. Some clarifications and additions to international humanitarian law may be required, but it will be difficult to future-proof them. Armed autonomous robots are indiscriminate and disproportionate weapons and we must treat them as such now. As such the United Nations should consider placing them on the prohibited list of weapons under the Convention on Certain Conventional Weapons. We rely on possible future technological fixes at our peril.

Autonomous systems: precautions in attacks

William H. Boothby

Deputy Director of Legal Services (Royal Air Force), London

Legal controversy over the use of unmanned aerial vehicles, drones, or remotely piloted aircraft, if I were to use the terminology now used by the Royal Air Force, to attack targets during armed conflict has been increased by comments such as those attributed to Lord Bingham¹. Reportedly likening current generation remotely piloted aircraft to landmines and cluster munitions, the noble Lord apparently said “It may be, I’m not expressing a view, that unmanned drones that fall on a house full of civilians is a weapon the international community should decide should not be used”.

When we consider these legal issues we must be careful to distinguish the law that prohibits certain weapons because of their nature from the law that regulates targeting decisions. Any weapon, whether it be a rifle, a manned fighter aircraft or an unmanned aircraft is capable of being used in breach of the law of armed conflict, for example, by directing it intentionally at civilians or by knowingly using it to prosecute attacks that it is appreciated will cause civilian losses disproportionate to the military advantage anticipated from the attack. Equally, mistakes in targeting decisions, technical malfunctions in guidance systems and so on can result in attacks which do not have the expected or intended consequences.

But the focus of the reported criticism seems to be the weapon as such, not the fact that it could be used inappropriately. We should, therefore, try to consider the legal issues that arise with the use of unmanned aircraft.

I would label the machines that we are talking about here Unmanned Combat Vehicles, or UCVs. Such vehicles operate in the air, land or maritime domains, they may be of any size and, crucially, they either carry

1. *Unmanned drones could be banned, says senior judge*, www.telegraph.co.uk, 6 Jul 2009.

and deliver to target lethal or non-lethal force, or they can use on board technology to direct to target force which has actually been deployed by another platform. The important factor from my perspective as a lawyer is the ability of the vehicle to direct a weapon to a target, whether it took the weapon there or not. For the purposes of this talk I am going to focus on the air version of such vehicles which I will call UCAVs (Unmanned Combat Aerial Vehicles).

Although unmanned, the vehicle will generally be controlled from a ground station, with a human operator at the controls, in the loop as the jargon goes, who would determine whether the machine is to be used to attack an object or person. There would not seem to me to be a qualitative legal difference between that decision and the decision of any other commander of a platform capable of remote attack. Either the operator has sufficient and sufficiently clear information to form a proper basis for his decision or he does not. Rather than legal in nature, the objections seem to me to be grounded in ethics, and can be summed up in the question whether it is proper for one Party to the conflict to use a method of attack free of personal risk and which kills and maims those in the target area. It is I suppose a development of the “bombing from 15,000 feet” debate during the Kosovo Conflict. As a lawyer, I satisfy myself with reporting that others have an ethical issue, noting in passing its apparent linkage with traditional notions of chivalry in conflict. As an international lawyer, I do not have any difficulty with man in the loop UCAV operations as currently understood and operated. They are plainly in my view lawful.

Let me now turn to the more interesting notion of autonomous attack. This activity, as understood for the purposes of this paper, consists of the launching of an unmanned vehicle which searches, usually in a pre-determined area of search, for objects that conform to pre-set algorithms recorded in the weapons control systems of the UCAV. When an object is observed by on-board sensors that so conform, the UCAV will reach its own decision autonomously on whether or not to attack the object. It is understood that this decision will be based on the accuracy of the match between what is observed and the pre-set data. Any such autonomous UCAV would be the subject of legal review in accordance with article 36 of AP1². Also the weapon that is used by the UCAV will itself need to be the subject of legal review in its own right. Such reviews are the

2. Protocol 1 additional to the Geneva Conventions and regulating international armed conflicts. Article 36 requires that all new weapons, methods or means of warfare be legally reviewed by states party to determine their compliance with the international law affecting that state.

responsibility, in the UK, of DCDC at Shrivenham. But we are considering the unmanned nature of the guiding vehicle and the legal issues that flow from its autonomous decision-making.

Any state considering acquiring technology of this sort must reach a legal conclusion on the basis of the international law applicable to that state, and its interpretation of that law taking into account the particular technology under review.

Autonomous platforms give computer based equipment the complex task of deciding what should be attacked, when the attack should occur, how the attack should be prosecuted, perhaps which weapon should be used, what the angle of attack should be, the altitude from which the weapon will be released in the case of an UCAV and so on. Let us be clear, there is no treaty, or rule of customary law, that specifically prohibits or restricts the use of autonomous attack technology. The autonomous decision making process must, however, be considered in the light of the targeting rules I mentioned earlier which regulate all attacks, autonomous or otherwise.

The legal principle of discrimination requires that the UCV must be capable of directing the weapon at a specific military objective and that the effects of the weapon shall be limited as required by the law. This rule means that if the UCAV's operation or control of its weapon is such that the weapon will strike military objectives and civilians or civilian objects without distinction, the rule is likely to be broken. If the vehicle has an autonomous attack capability, the person reviewing its legality is, therefore, concerned to establish whether the particular technology governing the vehicle and its prosecution of autonomous attacks is such that those attacks will properly discriminate between military objectives on the one hand and objects (or persons) that are not military objectives on the other.

Of considerable relevance will be the sensors, guidance technology and other facilities on the vehicle and the extent to which these will enable the platform to direct attacks at military objectives. Also important will be the way in which the vehicle is intended to be used, how missions are going to be planned, the battle space information which will support mission planning, the types of target which the machine will engage, the sorts of location in which it is planned to mount such attacks, the fidelity with which the sensors can identify particular sorts of target and so on. Any assessment of the legality of a proposed autonomous system will be informed, *inter alia*, by the sort of information I have mentioned and will judge whether the system is capable, in the general circumstances of intended use, of being used in a discriminating way. So, if the UCAV is to be used truly autonomously, the task will often boil down to determining

whether the available technology is capable of distinguishing the objects that constitute the targets the vehicle is designed or intended to engage.

A treaty to which the UK is party, but to which the US is not, sets out the precautions that must be taken in making attack decisions. So we must consider whether the equipment and its intended method of employment will enable the required precautions to be taken.

The precautions rules start by asserting that constant care must be taken to spare civilians and civilian objects. In and of itself, I am not sure that that rule takes us very much further. More specifically, however, the rules provide that those who plan or decide upon an attack are required:

to do everything practicable or practically possible to verify that the objective of the attack is a military objective.

Breaking off at that point for just a moment, it is likely that the algorithm-linked technology that allows the UCAV to achieve its military purpose will also enable it to comply with the legal principle. By this I mean that if the technology of the autonomous attack system does not place a person in the loop, that does not in my view mean that all uses of the system will automatically breach the discrimination rule. So, if the mission planners can, in advance of the mission, limit the timing, location and objectives of any UCAV attack and the weapons used, the algorithms, depending on their sophistication and reliability, may be able sufficiently to restrict attacks to objects appropriately recognized by the software as legitimate military objectives. By using such technology the principle of discrimination can be catered for notwithstanding that the attack was autonomously decided upon.

There are, however, additional precautionary rules. They require that those who plan or decide upon an attack must also:

take all feasible precautions in the means and methods of attack to avoid, and in any case to minimise, incidental civilian loss of life and injury and damage to civilian objects,

refrain from deciding to launch 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.

Furthermore, an attack must be cancelled or suspended if it becomes clear that the objective is not a military objective, or is subject to special protection, or that the attack may be expected to have disproportionate collateral consequences, and effective advance warning must be given of

attacks which may affect the civilian population, unless circumstances do not permit. Dealing with this last point first, if surprise is not a factor, a warning could of course be given. If surprise is a factor, however, the warning is not required by the rule.

Turning to the remaining requirements, each state must reach its own decision as to the legal acceptability of autonomous attack technology according to the legal rules by which it is bound. My focus here has been on the rules binding the United Kingdom (UK).

The introductory language in the treaty that binds the UK states, “With respect to attacks, the following precautions shall be taken” and the precautions which we are about to consider must be taken by “those who plan or decide upon an attack”.

The problem in relation to a UCAV with autonomous attack technology is that, when used in its autonomous attack mode, nobody decides upon nor plans the particular attack. In my view that does not mean that we can simply say that the requirement to take precautions does not apply to autonomous attacks. The deployment of the UCAV is likely to be reflected in planning decisions and commanders will decide when and under what circumstances the UCAV is to be operated. We must, therefore, in my view, determine whether the technology of the relevant unmanned system enables the precautionary requirements nevertheless to be satisfied. This might, for example, be achieved by ensuring that a person remains “in the loop” of decision making, is fed information as to what is going on in the target area and decides whether an attack, which may have been autonomously decided upon, proceeds or not. Alternatively, the UCAV system may provide for a person to monitor what is going on with a view to countermanding the machine’s autonomously reached attack decision where this seems to be necessary.

If truly autonomous attack is being considered, the remaining issue for us to consider is whether the UCAV is able to make the qualitative decisions provided for in the precautionary rules. I have in mind here, for example, and this is just an example, the determination whether an attack may be expected to cause disproportionate losses among civilians compared to the concrete and direct military advantage that is anticipated. There is at present, so far as I am aware, no known mechanical decision making technology that can address essentially qualitative factors, such as risks to civilians and the balance between risks to one category of individual and advantage to another. Those functions appear to require evaluations that may pre-suppose human involvement. Proper discharge of the legal requirement to take precautions may, therefore, require a person to be “in the loop”. But it may be possible at the *sortie* planning stage to take

precautions in attack, which will hold good throughout the period of UCAV search to an acceptable level of confidence. This may be the case with, for example, attacks on targets in areas remote from civilians and civilian objects. It may also be the case if the expected loss of civilian life, injury to civilians or damage to civilian objects can, for whatever reason, be identified with acceptable confidence at the *sortie* planning stage as being not excessive in relation to the concrete and direct military advantage anticipated from the attack of the target. If future developments in technology were to enable the machine to determine whether there has been material change of circumstances in the area of the planned attack, this may also assist us.

I stress that the application of the law will be informed by technology and, I suggest, in particular by established technological performance. If technology is developed which either is capable of making autonomous evaluative decisions or which is at least capable of contributing to such decisions to a degree that at least reduces the requirement for human involvement in them, the mere fact that it is a machine that is involved in that way would not in my view lead to the automatic conclusion that the legal precautions requirements had been breached.

The main issue for anyone concerned to determine the legitimacy of acquiring autonomous attack UCAV technology is whether the system is capable of being used in accordance with the principle of distinction. If fitted with suitable algorithm linked sensor technology, the answer is likely to be yes. The main issue for anyone planning to use such equipment on a particular occasion will be to ensure that any particular attack undertaken by the system complies with all legal requirements. Both will wish to be satisfied that the way in which it is planned to use the system and the capabilities of the system itself enable the precautions required by law to be taken.

The current technological capabilities of automatic target recognition, the prediction that the future conflict environment is likely to be cluttered and congested, and the legal requirements in attack I have outlined suggest to UK MOD that a requirement for man-in-the-loop operation of UCAVs will remain for the foreseeable future.

I am, of course, a lawyer and wisely perhaps hesitate to offer thoughts on ethics. Perhaps it suffices, therefore, for me to wonder whether, regardless of future technical capability, it can ever be ethically acceptable for a machine alone to decide who should be attacked and who should not.

Non-lethal capabilities – a double-edged sword

Richard Froh

Deputy Assistant Secretary-General, Defence Investment, NATO, Brussels

Why talk about non-lethal capabilities and non-lethal weapons? Why do we have them? They provide commanders options between presences which act as a deterrent – merely being there can sometimes stop a conflict or bring a situation back under control – and the use of lethal force. If they are not new – police have been using non-lethal weapons for years. Back when I was engineer Troop Commander in the Canadian Armed Forces, we were sent to guard the Toronto Airport during the 1976 Montreal Olympics. We had trained in the use of non-lethal capabilities, but we didn't have much of the technology I shall show you this morning – it didn't exist yet.



What I'll talk about during my presentation is, firstly, a little bit about terminology, so we are all talking about the same thing. A little bit of history as to what NATO has been doing including examples of non-lethal capabilities. Then I will link it back to the theme of the conference, the implications of new technologies on international humanitarian law. Finally, I will throw a few issues onto the table for discussion.

First, the definition of non-lethal weapons: one of the real advantages of NATO for the 28 Allies who are our members is providing a forum where we can agree on what we mean by certain terms. But it is not only the 28 Allies; we have extended this important work to include a number of partnerships. In Afghanistan – all 49 nations¹ that are contributing troops to the operations in Afghanistan are using NATO terminology and procedures.

Now, as you are all well aware it's impossible to guarantee that no death will result from the use of any weapon. My pen is a weapon, in the hands of a well-trained person, if you can believe what you see in

1. Since this presentation, Bahrain has joined ISAF, making a total of 50 troop-contributing nations.

movies or on TV; so virtually nothing is non-lethal. What we are looking for are weapons or capabilities that can reduce the chance of lethality or even long-term incapacity. Terminology here is limited to the agreed NATO definition for non-lethal weapons (Graph 1) as other terminology related to lethal weapons has not been fully accepted for the very reason I have just talked about. We talk about less than lethal weapons, we talk about non-deadly weapons, we talk about compliant weapons, and we talk about pain-inducing weapons. In reality, and I think I shall be able to show you that we are talking about more than weapons. A number of the technologies we have do not fall under the traditional sense of weapons. A weapon is an arm, an armament, and/or its ammunition. Many of these are not weapons but other things that allow us to incapacitate a potential enemy, perhaps even to incapacitate civilians, so we can safely separate them from the potential enemy.

	<h2>Non-Lethal Weapon</h2>
 <p>A weapon that is explicitly designed and primarily employed to incapacitate or repel persons, or to disable equipment, while minimizing fatalities, permanent injury and damage to property and the environment (AAP-6)</p>	

Graph 1 - Non-Lethal Weapon

Now, I talked about capacity capabilities and why we use that term. We don't have a formal agreement on this definition (Graph 2) but it is being used by experts in our working groups on non-lethal capabilities. Pictured here is a light-emitting diode (LED) which temporarily blinds, disorients and the manufacturer says it can actually cause vomiting, thereby incapacitating someone.



NATO
OTAN

Non-Lethal Capability

A capability **specifically** designed to achieve a relevant military effect on a person, equipment or infrastructure yet with a **significantly lower risk** of human fatality or permanent injury or undesired damage to infrastructure than could be expected from conducting the same task through the use of conventional lethal systems. (Working Definition)



Graph 2 - Non-Lethal Capability

NATO's involvement in this area (Graph 3), as with many things at NATO, changed after the end of the Cold War. In 1991, we had our first strategic concept. Before that it was perhaps easier – we knew



NATO
OTAN

NATO Involvement

- 1994 - role of NLW in Peacekeeping and Support
- 1999 – NLW Policy and Defence Capabilities Initiative (DCI)
- Research and Technology Studies
- Defence Against Terrorism POW
- Armaments Groups

Graph 3 - NATO Involvement

who the enemy was, we did contingency plans to fight them. I did two tours in Germany with my Engineer Regiment. We knew where we were going to go when the balloon went up. We exercised the plan regularly. But after 1989 it was no longer as clear what NATO's new role was in ensuring peace and security in the North Atlantic Region.

So, in 1994, following on from that strategic concept, NATO tasked its armaments community to look at non-lethal weapons and capabilities to identify what benefit they could have. Of course, the media played a big role here by identifying casualties, being aware of events in a crisis or in a theatre of operation, through almost minute to minute reporting of activities. The tolerance of casualties, in particular of non-combatants, was very, very high and the lethality of weapons became a very sensitive issue.

In 1999, at NATO's 50th anniversary Summit in Washington we launched an initiative called the "Defense Capabilities Initiative or DCI" and non-lethal weapons (NLWs) were one of 58 capabilities that were being pursued. We have a research and technology organization in NATO that is made up of about 3500 experts, from government, academia and industry. They did a series of studies on NLWs, thereby improving our understanding of them. A non-lethal weapon effects assessment was done. Non-lethal weapons were seen as useful in future peace-keeping operations. They identified a number of areas that needed to be looked into further – radio frequency devices and anti-traction approaches, rapid barriers, stun devices and nets. The experts also looked at the human effects of non-lethal capabilities. All this work will allow us to go back and assess how well we are complying with international humanitarian law.

In 2004, shortly after the Madrid bombings, we launched a defence against terrorism programme of work. One of the eleven items on that programme of work was non-lethal capabilities. It is being led by Canada – a very big demonstration, in fact, the wrap up demonstration, will be held in Ottawa next month. Canada and the US are jointly hosting this event. Within NATO the Conference of National Armaments Directors (CNAD) has the lead. The NATO Army Armaments Group has a non-lethal capability working group that has worked very closely with experts on military operations in urban terrain, or fighting in built-up areas. That is because that's where non-lethal capabilities (NLCS) are going to be used the most, that's where the civilian population are, and that's where we need to be able to incapacitate but not permanently injure or worse kill someone.

Here are some categories we have identified for NLC. As you can see, there's a wide range of non-lethal capabilities fielded or under development. Some of them you will recognize as weapons (like the gun in the bottom left) but others, like slippery foam, are not weapons at all. Pepper spray

(at the top right) is actually a chemical agent and the truck mounted high powered microwave emitter (bottom right) is similar to electronic warfare but has different targets. Of course, electronic warfare has been used by military forces for years against enemies as a legitimate force multiplier on the battlefield. Electromagnetic weapons are lasers, the use of light – dazzlers as I showed you earlier and high-powered microwaves. Chemical NLC include obscurants like smoke, malodorants (things that smell so bad that you don't stay around for long), anti-traction foams and calmatives (to calm down a group or perhaps even to put them to sleep). Acoustics include ultra sound – I don't know if you realize as we grow older our ability to hear higher frequencies goes down, and so when McDonald's in the UK were having some problems with young people hanging around outside their stores and getting into trouble, they installed ultra sound emitters that people like me would never hear, but an 18-20 year old would and the result was they moved away from the stores. Stun guns and other forms of loud noises are a non-lethal way of breaking up a crowd.



Mechanical means, such as caltrops, take us back to the Roman times – these are sharp triangles we can put on a road to stop people on foot, on horseback or in a vehicle from going down a road. Spike strips and airbag mines can do the same thing. Blunt impact weapons, such as bean bags or water cannons can be effective against personnel. And last but not least, there are ancillary technologies. Here we are talking about marking dyes so you can mark instigators of a riot to prove they were there. We can also use non-lethal casings for our ammunition so those casings cannot be used against our troops later on.

Non-Lethal Capabilities have a range of uses shown here (Graph 2). The traditional one, of course, is crowd or riot control – remembering that the military is the force of last resort. Normally, the police have the responsibility for dealing with unruly crowds. Sometimes, the Gendarmerie could then step in and then, as a last resort of course, the military. The next three uses are closely related to that, again when we're working in areas where there are a lot of civilians. Discrimination of them will allow us a way of dealing, protecting our soldiers, doing the mission we need to do and not having to resort to lethal force against innocent people. In hostage situations, your aim is to save the hostages. You don't succeed in your mission if your hostages don't live. So, what you want to do is incapacitate the people holding them. And last but not least there is counter piracy. Just yesterday morning I flew from the Seychelles where I attended an international conference on counter piracy. The international community's response to pirates should include giving merchant ships and our Navies, non-lethal ways or less lethal ways of responding to pirates.

The relation of all this to international humanitarian law as I read it, and here I am not an expert, is that NLC provide a means of protecting against unnecessary human suffering. The Geneva Conventions, their supplements and the specific rules going back to the 1868 declaration on renouncing the use, in time of war, of explosive projectiles under 400 gr. in weight, are the result of long standing concerns about how to restrict the use of certain weapons.

These laws affect all aspects of military operations, both traditional and non-lethal. It's interesting that non-lethal is not specifically mentioned in any of these conventions or rules, so one must assume that NLW must be held up to the same standards as other weapons. That said, chemical weapons have a specific status in international humanitarian law and I'll come back to that a little bit later, as do lasers and anti-personnel land mines.

Let me now flag up a number of issues (Graph 4) – hopefully to feed our discussion which will follow. Our work on NLC will give us new weapons which will need to be evaluated by nations to ensure that they comply with international humanitarian law. I found it interesting that the first speaker this morning spoke about the US testing all their weapons to find out if they comply or not. All nations have that responsibility under international law. We have run into some ethical issues, as we were doing

	NATO + OTAN	<h1>Issues</h1>
<ul style="list-style-type: none">• Duty of nations to evaluate compliance• Public understanding and acceptance• Use of Chemical Agents• Lasers• Lower threshold for use of force 		

Graph 4 - Issues

some of our studies, as to how to determine the effectiveness of these non-lethal capabilities. Medical people, by their training, find it difficult to work on something which aims to incapacitate – it's better than killing but it is still not what people went to medical school for.

There are issues with NLCs. The death of a man in Vancouver after the repeated use of a teaser, and a 2003 incident in a US disco, where the police or the building's security people used pepper spray on two people in a fight, panicked other patrons, resulting in over 100 people being killed in the crush to get out, are examples where the use of a NLC resulted in a lethal result. So, non-lethal capabilities have gained a bad reputation for much of our public. I think a lack of understanding of just what it is they really do may be behind this. When discussing non-lethal weapons and capabilities, chemical weapons probably present the greatest problems. As I understand the Chemical Weapons Convention, this class of weapon is not to be used in armed conflict but they can be used in crowd control operations. So, it often depends on how you use them and where. The result is that our progress in developing such weapons has been very slow. I welcome the work of the International Institute for Humanitarian Law and discussions such as we are having at this conference, as a way of filling that knowledge gap.


Lasers have many military uses for targeting. In using them, we have to be careful to ensure that they are not causing permanent damage to individuals in a conflict zone, to avoid that they then fall under the specific agreement that was done to prevent the misuse of lasers.

You will remember that on my first slide, I presented non-lethal capabilities as a double-edged sword. I say this, because they give the commander another type of weapon to use in a given circumstance – if you like – another club in his or her golf bag. But by having it available, results in a lowering of the threshold to use force. Because you've got it you feel you must use it. Therefore, perhaps the escalation in the use of force is faster. Sometimes, insurgents or criminals knowing that a weapon will not kill them, will be braver. If you tell them it's nothing or we are going to shoot you, it causes them to think a little bit harder before provoking a reaction. If they know that you have something in between presence and lethal force, they may just push you to the point that you must use it, thereby taking control of the situation.



And then there is the question that: if you use an incapacitant on the battle field and, therefore, prevent your enemy from being able to act against you, then what do you do? Some might decide that, to make sure that they don't have to fight the enemy again later, they should act

to take enemy out of the battle permanently – I don't have to tell this audience, that such action is completely against international humanitarian law. Therefore, the training of the individuals on how to use these new weapons, including ethical training – so they use them correctly – is absolutely a key factor.

Now, here are some areas where we need to do further work (Graph 5). We need to continue to work on our terminology. The testing of these

	<h2>Where next?</h2>
<ul style="list-style-type: none">• Terminology• Testing• Training• Guidelines	

Graph 5 - Where Next?

	<h2>Other NLC</h2>
<p>We are not the only ones to have Non-Lethal Capabilities or to use Chemical Weapons</p>  <p>Questions?</p>	

Graph 6 - Other NNL

weapons needs to be done and here NATO could assist nations to meet their obligations under international humanitarian law. We can also provide them with a forum for discussing latest developments in the NLC field. Last but not least we need to develop guidelines for the use of non-lethal capabilities.

Let me just end (Graph 6) by saying that while inhumane use is a key criteria under international humanitarian law for judging a weapon, humans are not the only ones to possess non-lethal capabilities or chemical weapons – skunks are also very effective in their use!

V. Cyber warfare

Operational reality of cyber warfare

Herb Lin

Chief Scientist, National Research Council of the National Academies,
Washington D.C.

This presentation addresses some of the basic technical and operational realities of cyber conflict and cyber warfare. The primary source documents for this presentation are two unclassified and freely downloadable reports of the U.S. National Research Council: *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* and *Proceedings of a Workshop on Detering Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*.

To begin, there are three elements of an offensive operation: access, vulnerability and payload. Access is how to get at the system of interest; vulnerability refers to a weakness in the system of interest that the offensive party can take advantage of; payload describes what actions are to be taken once the system of interest has been penetrated.

Access takes advantage of the fact that computers have to interact with the outside world in order to be useful. A computer in a sealed metal box with no cables coming out of it is completely secure, but it is not very useful to anybody. For it to be useful, it is necessary to be able to put information in and to get information out (where the information in question can be programs or data or both). Gaining access is all about compromising any of the ways of getting into a computer.

Vulnerability is a weakness in the system. On a file cabinet, vulnerability might be an easily picked lock on the file drawers. Such a lock, for example, might have only two pins and be easily picked with a paper clip. A stronger lock might have 6 pins.

The payload specifies what to do once inside the computer: delete files, erase everything, steal information out of it, and so on. There are many things to do once inside the safe.

There are many means to gain access. Often, a computer is connected to the Internet, and it may be possible to use the Internet to gain access.

Access at a distance is called remote access. However, there are ways of getting at computers that do not depend on the internet. For example, with a USB key it is possible to infect a computer with a malware or, through mail order, a malicious person could easily change some software or put a new chip in it. The latter scenario is probably unlikely, unless you have stars on your shoulder. There are also social ways of gaining access—for example, by bribing a secretary to obtain access to the computer rather than by breaking through any security surrounding it.

There are two types of offensive operations in cyber space namely, attacks or exploitation and both are hostile. An attack is something that does something destructive. An attack actually destroys, degrades or disrupts information or the computer system or network. It is also possible to tamper with the integrity of a computer. For example, data can be changed or authenticity can be compromised by pretending to be somebody else or by an unauthorized use or by making the computer unavailable for somebody. Attacks are techniques for doing something to a computer so that somebody else cannot use it for its intended purposes.

Exploitation is going in a computer in order to get information out of it or “steal” it. It has to be emphasized here that this is not really stealing information. Indeed, if somebody steals a wallet, this person will have the wallet and the owner will not. However, if somebody steals information or credit card numbers, the owner still has its credit card number and the burglar has it too. So when I refer to the stealing of information from a computer, I really mean it in the second sense of the word. Both the pirate and the computer’s owner have it. In this way, somebody else other than the computer’s owner can have the information contained in it, without anybody knowing it. That is dangerous.

Attack and exploitation in cyber space use the same technical means to get at the information, to operate, to do what they want to do. They both have to gain access and to take advantage of vulnerability. To the victim, it all looks the same. It is impossible to know what is going to happen until the payload executes. So if somebody penetrates a computer system, nobody will know why they are there until something actually happens. To the news media it also looks the same. Everything is treated as a cyberattack, even if it is mostly exploitation. Although Stuxnet is a prominent exception, nearly all cyberattacks reported in the media are really exploitations.

Here are some of the key characteristics of offensive cyber operations.

The indirect effect of a cyberattack may be the primary intended effect. What is central may not be the computer itself, but the generator connected to the computer. The goal is to kill the computer so that the generator can

be killed. This means the effects of a cyberattack can span an extremely broad range as it is possible to hook up anything to a computer. An attack can be very targeted or very broad, depending on what the computer is connected to.

One can regard a cyberattack as a methodology that is similar to chemical explosives. A bullet uses chemical explosive and a ten-thousand pound blockbuster bomb uses chemical explosive. They have very different kinds of effects, but they are both chemical explosives. Similarly, cyberattacks have to be thought about as a methodology or as a way of conducting some operation or achieving some effect. There is a large range of available options when doing a cyberattack, just as there is a large range of options when using chemical explosives. The time and spatial scales for cyberattacks, for example, can vary over many orders of magnitude.

Cyberattacks are unattributable under many circumstances – that is, the party originating the cyberattack cannot be identified with high confidence under such circumstances.

The last point here is a fundamental reality: offense will always beat defense in cyberspace given enough time. This means that it is impossible to erect a fool proof defense. It is a completely offense-dominated environment for reasons that, for the purpose of this text, will not be discussed here.

Technology for conducting offensive operations in cyberspace can be obtained anywhere, by mail order for example, and the knowledge needed to conduct some kind of cyberattack is available on the internet. Thus, many non-state actors – companies, teenagers, terrorists, patriotic hackers, organized crime – can have influence and are sometimes able to cause some of the effects that large state actors can cause.

But not all, since large scale state actors still have many advantages in attacking that non-state actors do not. It's highly implausible that a single teenage hacker could bring down the entire power grid of the United States, but less unrealistic to consider that a hostile nation could be able to achieve this effect.

Because cyber technology is easily accessible, ascertaining an adversary's capabilities will be very difficult. This is particularly relevant when it comes to verifying agreements aiming at limiting attacks.

Cyber operations can be intended to affect a very broad spectrum of targets or be very narrowly targeted. Being more selective implies a much more highly targeted intelligence, as well as a lot more intelligence information. For example, one could target a very specific computer; such a task might require its serial number, and it would require a lot of effort and intelligence to obtain such information. Nonetheless, an important point to

mention is that nation-states have very few military incentives to conduct broad spectrum attacks as opposed to highly selective ones.

Success in cyber warfare depends on good, detailed, timely intelligence. Small details in the configuration could mean the difference between success and failure. For example, how do you know whether this computer is connected to that computer? There may be a cable, but no satellite intelligence will ever be able to confirm it, but without knowing, you may not be able to reach the second computer.

Concerning collateral damage, which is a big deal in international humanitarian law, it is very hard to estimate when talking about cyber warfare technology as the physics of the weapons do not help. Indeed, there is no physics to help you determine what the lethal radius is. Geography does not help, because the computer can be connected to a person half way around the world. Limitations on intelligence that might reduce the likelihood of success of a cyberattack may also be constraining.

Collateral damage is very hard to estimate. The accuracy of such an estimate depends strongly on the adequacy of the intelligence information, which is often harder to obtain than for kinetic targets. On the other hand, collateral damage from kinetic operations can also occur when there is a lack of intelligence.

For example, imagine that somebody seeks to use a cyberattack on a generator because that generator powers the Ministry of Defense. Unknown to the attacker, the generator also powers a hospital next door. A cyberattack on the generator may accidentally turn off power to the hospital. A kinetic attack on the generator may have the same result, because the intelligence was similarly limited. But a bomb used to destroy the generator is much more likely to kill people standing nearby—which suggests that under some circumstances, a cyberattack might incur less collateral damage, at least locally.

Cyberattacks can sometimes be used only once or few times, because the adversary sees the attack and he fixes the problem that enabled you to get in at first, so now you need to find a new way to get in.

Cyberattacks are likely to be most useful in the early stages of conflict or as covert action not associated with overt kinetic conflict.

Uncertainty in cyber warfare is a dominant and real issue. Attribution of an attack or exploitation can be very hard, although it is not impossible under some conditions. If the attack techniques used have never been used before; if the attacker has left no clues behind; if he has maintained perfect operational security and no one else knows; and if his motivations are unknown. If all of those conditions are met, then it will be very hard or practically impossible to figure out who attacked. However, some of these

conditions do not always hold and sometimes mistakes are made. You cannot count on that, but a lot of the things that are attributable come from the fact that mistakes were made.

In order to define cyber warfare, warfare in general needs to be defined. There are many different definitions of it. Nevertheless, there are still common elements shared among those competing definitions, namely that international armed conflict has to be state-organized, has to have military forces involved and has to be more intense than a mere border incursion.

Drawing upon these common elements, here is my working definition of the concept: cyber warfare entails a state cyberattack against the cyber assets of another state. By that definition, here are some things that are not cyber warfare: a teenager defacing a military website or stealing bank money from a defense contractor; stealing plans for a new jet fighter; terrorists groups using the internet for propaganda and recruitment; one nation stealing an economic business plan from a competitor in another nation to help its own businesses; an offensive military operation in which computers are used as supporting elements.

Here are a few examples of cyberattack: the destruction of a network or system; the personification of the command authority on the network to issue fake orders; data alteration; denying service; preventing people from communicating with each other; and so on. There are lots of interesting things to do.

How could those offensive capabilities be used?

For example, they could be used for defensive purposes. An early warning of an impending cyberattack might improve the prospects for defensive success. But the only way to obtain tactical warning of an upcoming cyberattack is to be able to monitor what a potential adversary's computer is doing and just before the attack is launched, the monitors signal us of that fact. Those monitors have to be living on the adversary's computers to be effective. A pre-emptive attack on the adversary's computer may also be possible. These approaches were suggested by Mike McConnell, a former director of the National Security Agency of the United States, in a Washington Post Editorial in February 2010.

Another way to answer could be by disrupting an attack in progress, which consists in launching a cyberattack to disrupt the attacking computers.

After an attack, there is a need for forensic investigation, which is necessary to know who has attacked. Such investigation requires offensive capabilities because it is often necessary to work a way back in the chain of computers controlling other computers in order to figure out who attacked. This implies some sort of intrusive capability to identify who is

attacking. Finally, it could also be possible to retaliate to discourage further attacks.

Of course, it is also possible to conduct offensive operations in cyber space for non-defensive purposes. For example, one could decide to go after an adversary air defence system. The rumour is that the Israelis disabled a Syrian attack air defence system, using a cyberattack. Somebody else might want to go after an electrical power grid that powers the Ministry of Defence or to influence the outcomes of a foreign election by attacking and hacking their electoral voting machines. I am not advocating any of these things, I am saying this is the sort of things that could be done.

Concerning cyber exploitation, there are some basic facts to consider. Exploitation is essentially espionage, which is done by all nations and does not violate traditional interpretations of international law. It is often called cyberattack, but it should not be. If every reference to cyberattack in the newspapers that are really exploitation were eliminated, there would be many fewer stories. The problem here is that talking a lot of cyber exploitation as attack results in a very rhetorically charged and political tensed atmosphere. That is what should be expected and that is what is happening.

Concerning the challenges met by the international legal regulation in cyber warfare, here is an incomplete list.

- Difficulties of attribution – attribution is not impossible in all cases but it is very difficult to do.
- The ease with which you can operate outside of national borders. If a national of nation A goes to nation B in order to conduct its attack on nation C, who is responsible at that point? Furthermore, what are the legal challenges in terms of determining responsibility for non-state actors?
- Cyberattacks are inherently stealthy. Cyber warfare can be compared with submarine warfare, because submarines too were stealthy. Cyber warfare can be seen as the equivalent of submarines in cyberspace.
- The intermingling of civilian and military infrastructure. For example, 95% of American military communication goes through a civilian infrastructure.
- Distinguishing between exploitation and attack. Is it based on the idea that exploitation is legal and attack is not? In the same line of thoughts, how does the attacker or penetrator let its adversary know what is happening? By calling and saying: “the next thing you see is going to be an exploitation”? No, now the element of stealth has been lost.
- Distinguishing between an active defense, which is responding to an attack in the cyberspace, and another attack that is not a response? What

does happen in the case of a delayed attack? If a penetration is set up in September, but the explosion in cyberspace happens in December and destroys the computer only then, when was the attack and what laws govern that?

- The private sector has the capability of conducting offense of operations, but the laws prohibiting it are not necessarily effective.
- There is the virtual impossibility of imposing meaningful controls on the acquisition of offensive capability in cyberspace. As far as I can tell, all the international humanitarian law issues relate to the use, nothing has anything to do with the capability itself and how you regulate the capability, which is impossible for a variety of reasons.

I would like to emphasize once more that this was an incomplete list.

Cyber warfare: is there a need for new law?

Matthew Waxman

Associate Professor, Columbia Law School, USA; Adjunct Senior Fellow,
Council on Foreign Relations; Member of the Hoover Institution
Task Force on National Security and Law

My topic is “Cyber Warfare: Is there a Need for New Law?”, and I would like to address it in terms of three sub-questions. First, with respect to cyber warfare, is there a gap in international law, and if so does that pose an international legal crisis? Second, what are the challenges to interpreting existing law or developing new international law in this area? And, third, what might the future hold with respect to international legal development and cyber warfare?

Let me begin with a preliminary note about what I mean when I refer to “cyber attacks”. Definitions of that term vary widely, and the range of hostile activities that can be carried out over information networks is immense, ranging from malicious hacking and defacement of websites to large-scale destruction of military or civilian infrastructure that rely on those networks. By “cyber attacks”. I mean efforts to alter, disrupt or destroy computer systems or networks or the information or programs on them, which is still a broad category. That breadth – encompassing activities that range in target (military versus civilian, public versus private), consequences (minor versus major, direct versus indirect), and duration (temporary versus long-term) – is part of what makes international legal interpretation or regulation in this area so difficult with respect to *jus ad bellum* and *jus in bello*.

With that in mind, *is there a gap in the law, and is it a crisis?* On the one hand, this is a very new problem. The information technologies involved are new and changing constantly and rapidly, and our dependence on information technologies and their networked architecture creates new security vulnerabilities. This raises difficult questions such as when might attacks on informational infrastructure using only bits and bytes of information – electronic ones and zeros – give rise to a right of armed self-defense, or during the course of armed conflict when might such

actions violate precautionary targeting requirements or constitute grossly disproportionate civilian harm?

On the other hand, though, this is a very old and common legal problem. That is, it has always been possible to wage conflict using means other than kinetic violence, and there has long been much debate and disagreement about how and where to draw such lines. During the Cold War, for example, much debate centered on questions about when the use of economic power or political interference in another state's affairs violated international law or could give rise to the right of self-defense. Ancient methods of conflict like sieges and modern ones like strategic air bombardment have prompted questions about the limits on means of warfare that have indirect (or sometimes very direct) and very devastating effects on civilians.

In that regard, cyber warfare emerges within a legal framework that goes back centuries, with significant refinement and codification in the 20th Century. As to *jus ad bellum*, we look primarily to the UN Charter, including Article 2(4)'s prohibition on the use or threat of force, and Article 51's recognition of self-defense rights. As to *jus in bello*, there are treaty instruments like the Hague and Geneva Conventions, though much of that regime boils down to the core principles of necessity, distinction, and proportionality.

As new technologies arise, of course, they present translation challenges for these bodies of law. They always have. During the last century, such conflict methods as proxy conflicts through support for insurgencies, counter-insurgencies, and terrorism, as well as forms of economic strangulation or political subversion, raised tough questions about legal categories and boundaries. During the first Gulf War, the coalition air campaign destroyed Iraq's dual-use electrical power system, which degraded Iraq's military capacity but also resulted in widespread and long-term civilian deprivations, therefore, raising questions about targeting distinction and proportionality. In the course of Kosovo air operations, NATO forces bombed Serbian television and radio stations on the grounds that these information systems were integral to Serbian war-making capacity, again raising questions about how to classify and assess legally such targeting.

Cyber attacks and cyber warfare undoubtedly present new and perhaps more difficult legal translation problems. But the point of these historical examples is to show that these challenges differ more in degree than in kind from previous legal challenges. The law may not be as clear or as effective as we would like as we try to map cyber warfare onto it, but cyber warfare is not emerging in a gaping legal hole or creating a new legal crisis.

That is not to say that there are not *new challenges to refining the law or developing new law* with respect to *jus ad bellum* and *jus in bello* of cyber warfare. Some of those challenges include:

- Substantive understanding of cyber attacks and threats: some states want to preserve the flow of information, while others want to be able to disrupt and control it, and powerful states have varying views on cyber security because of differences in international political systems and relations between the public and private sector.
- Identification challenges: it may be difficult to distinguish in real-time between offensive and defensive actions, or hostile attacks versus intelligence activities in cyberspace.
- Verification problems: it will be difficult to monitor, detect, and substantiate violations of norms in this area because of technical and jurisdictional limits.
- Attribution issues: thorny issues will arise as to whether and when actions by private individuals or groups in cyberspace may be attributed to a state – both as a matter of forensics in linking cyber activities to their human perpetrator and as political matter in establishing the level of state control or sponsorship.
- Secrecy: Not only will states be very reticent and guarded over their offensive and defensive actions, they will also be reluctant to disclose information about attacks they might suffer or repel, for fear of compromising intelligence capabilities or exposing vulnerabilities.

An upshot of this set of challenges is that new comprehensive treaty or interpretive consensus of existing law is unlikely anytime soon in this area (at least absent a catastrophic event). We may continue to see agreement or refinement of multilateral treaties that deal with specific pieces of the cyber-security problem, like the International Convention on Cybercrime, which requires parties to develop criminal laws against hacking and other illicit cyber activities like computer fraud. Or we may see policy agreements among small numbers or subsets of states, like a NATO strategic concept with respect to cyber defence or joint declaration among like-minded states that seek to block information activities they view as subversive.

New treaties are a long way off, though, unless the states elevate form over substance, and they negotiate and adopt treaties with vague language that papers over differences and merely restates the toughest questions

So, if this prognosis is correct, it leads to my third question: *what will the future look like with regard to law in this area?* In short, we are likely to see law develop not through negotiation of comprehensive treaties but through slow and uneven development of state practice.

This process could be even slower and more uneven than in past eras of radical transformation in the technology and mode of conflict, though, for several reasons related to the challenges outlined above. To an even greater degree than prior forms of warfare, cyber warfare may lack clearly discernible starting points and readily observable or provable actions and counter actions. This does not mean that legal line-drawing through UN Charter and IHL interpretation or new international legal agreements is impossible with respect to issues like prohibited attacks and self-defence. It does mean, however, that while information technology continues to evolve at faster and faster rates, the processes of claims and counterclaims toward a predictable, stable outcome, or the accretion of interpretive practice commanding broad consensus, will likely be slow and uncertain.

This legal evolution will occur less through formal negotiation, and more through posturing and policies to advance particular interpretations by states, international organizations, and other influential actors in the international system – that is, through a process of translating old law to meet new challenges, or what Michael Resiman describes as “a process of counterclaims, responses, replies, and rejoinders until stable expectations of right behaviour emerge”. Examples of this that we are seeing include US declaratory policies with regard to self-defence; the drafting of the Tallinn manual on international law applicable to cyber conflict, and reactions by states to it; the upcoming London diplomatic summit on cyber security; and diplomatic discussions among China, Russia and other states about appropriate international responses to cyber threats.

In sum, (1) many issues of cyber warfare are at the same time technologically unique and novel yet also legally familiar and historically recurring; (2) some particular characteristics of cyber attacks – including the low visibility of attacks and counter-actions, likely disputes about key facts, and difficulties in establishing attribution – will make it especially difficult to build legal consensus in assessing real-world scenarios; and (3) therefore, for the foreseeable future, states will have to pursue offensive and defensive strategy within existing legal frameworks regulating force, with an eye toward incremental interpretive evolution through state practice.

How to integrate cyber defence into existing defence capabilities

Suleyman Anil

Head, Cyber Defence Section, Emerging Security Challenges Division,
NATO Cyber Defence Coordination & Support Centre, Brussels

The aim of this presentation is to provide you with an update on cyber defence activities and developments that NATO is involved with. Obviously, the following presentation represents my views as a member of the international staff and not those of the organization.

Before going any further, a few words on the division where I work at: the Emerging Security Challenges Division. Our Secretary General, Prime Minister Rasmussen, decided to create a sixth division in the NATO HQ last year. International staff from other divisions were selected and moved to create the new division. The division has been operational since August last year and functionally aligned with the new challenges that the Alliance is expected to face in coming years as identified in the new NATO Strategic Concept.

Cyberspace is recognized by many as a new global domain, created by humankind. A study made by NATO compares cyberspace to air, maritime and space, all natural domains. The most interesting characteristics of cyberspace is the fact that it encompasses all of the other global domains. Today, in the informatics age, none of the natural domains (air, maritime or space) can function if cyberspace fails which would mean going back to the time of the messenger pigeon.

We all need a trust in the cyberspace. The military-civilian separation in cyberspace does not exist. Information infrastructures are the same: 95 per cent of world data and voice traffic is carried over fibre optic cables, providing shared bandwidth services to both public and private sectors. Dedicated data links are minimal and only for contingency purposes with limited capabilities which cannot sustain full scale services.

I am an electrical engineer by education, but I am told by my colleagues dealing with structural engineering that a structure will lose its initial purpose if 37% of it is physically destroyed. Theory suggests that the same

principle would apply in modern structures such as this one if 37% of its cyber infrastructure was destroyed. What is more for the cyber parameter is that even the behaviour of the whole structure could be manipulated if the information infrastructures of the structure were compromised. This brings up an interesting question concerning the choices between kinetic and non-kinetic options if the functioning of a structure is required to stop or be different during any conflict; political, social, industrial or military. In one of his recent speeches, our Secretary General has put this in very simple terms. A trusted cyberspace is a must for all services, be it public or private.

In 2010, a group of policy experts from various NATO states, led by Mrs Albright from the United States, prepared a report for the Secretary General, in preparation of the new NATO Strategic Concept, addressing the new challenges that the Alliance would be facing in the next ten years. The report identified the three most probable threats as cyber assaults, along with ballistic missiles and international terrorism.

So, what is NATO doing about addressing the cyber threats which are rapidly growing both in numbers and in sophistication? The new Strategic Concept, approved by Heads of States and Governments, has placed the emerging security challenges, which includes cyber defence, under the collective defence task of NATO. It further stated that cyber attacks can reach thresholds where national security or stability of a member state may be threatened. This is the first time cyber defence is integrated in such documents. NATO does not have plans to create an offensive capability. Its current effort is to build cyber defence measures to protect all networks in NATO and assist the member states when requested.

Heads of States submitted more specific tasks at the summit of Lisbon, in November last year, which resulted in the statement on cyber. Concerning this summit of Lisbon, it is important to underline that cyber defence has always been addressed in the NATO's summits since the 2002 Prague Summit, but never in this detail and at this level of ambition. Since November, a significant staff and committee time and resources were dedicated to prepare a policy and an action plan to meet the objectives set by the Heads of States and Governments.

As a result, in June this year, Defence Ministers approved the new NATO Policy on Cyber Defence and an action plan for the implementation of the new policy has been elaborated. The new policy is a revised version of the previous one, which was developed following the cyber attacks against Estonia, a NATO member state, in April/May 2007. Since the approval of new policy and action plan, we are now in the implementation phase of the action plan, which will continue for the next few years.

So, what is new in the June Cyber Defence Policy? What is the difference between this policy and the previous policy of 2008? The new policy maintains the majority of elements of the previous policy, but goes further in underlying the significance of cyber defence with respect to modern warfare and aims to integrate cyber defence in all levels of NATO business processes in place to execute core tasks of NATO. NATO's core tasks are described in the Strategic Concept as Collective Security, Crisis Management and Cooperative Security through partnerships.

The policy and action plan is being executed right now. Regarding the collective defence, NATO Defence Planning Process (NDPP) will identify for each member States the defence capabilities and the measures that should be in place and which can be put under NATO's collective defence when necessary, when required. The resilience and the prevention capabilities will be made under NATO's own infrastructures. Indeed, NATO implements and operates its own informational infrastructure. It does not rely on the member States' infrastructure. From North America to Afghanistan, from Norway to Turkey, there is an information infrastructure where NATO's business classified operations, command, control and consultation are performed. That informational infrastructure has to be maintained in its integrity to ensure that NATO can meet its objectives. Informational intelligence sharing, specific to cyber defence is another compound. We are integrating cyber defence into NATO's intelligence sharing processes and committee work. Furthermore, NATO also runs annual exercises to exercise what is in them obviously.

The second core task, namely, crisis management, is a response capability during crisis or incidents. NATO runs its own, which is traditionally known as, Charter Computer Emergency Response Team. It has been operational since 2006. Until the end of next year, we will enhance capabilities, which is really about detecting the cyber attack and responding to it and, of course, taking the necessary measures. In crisis management procedures, cyber defence is being integrated into the NATO existing crisis management procedures and manuals. Tactical information-sharing, which is in real time or incidents or field specific, aims at enhancing information-sharing capability in these areas. Concerning the exercises, NATO has been running for the last three years annual cyber defence exercises. In addition, cyber defence is also being integrated into crisis management exercises and some of the other military exercises.

Corporative security is about partnership with the NATO partner countries. For those who are not familiar, NATO has partnership programs with more than 40 countries from all over the world: Japan, Korea, Australia, New Zealand or Central Asia, Balkans, Northern Africa,

the Middle East. There are several programs, from science for peace programs to technology agencies working with the partners to exercises made in collaboration with the partners. As a consequence of these programs, cyber defense will be further integrated in the corporative security process, using the leverage of the partnership in the global threats. And partnerships are also in other areas. They are a tailored approach. Depending on the partners and the political positions, the cooperation and the support may vary.

In conclusion, the challenges in cyber defense, or warfare, or security are numerous. It starts with a lack of cyber culture or some would call it norms of behavior. Cyber technology is very young and that is why cyberspace is dominated by criminal groups.

Then there is a lack of international cooperation. Professor Lin made a very good point about attribution. Even though he stated that the attribution was impossible, his point was clear. It is impossible only if specific and exceptional conditions are met. Therefore, one cannot conclude that attribution is impossible. The biggest obstacle in attribution is the lack of international cooperation. In most countries, especially western countries, at the national scale, the attribution problem has been minimized and it is getting better every year, because there is enough legislation in place or regulations and there is a national cooperation between the service providers, telecom operators, and law enforcement. This means that for an incident that remains in the boundary of one nation, the attribution problem is minimal. The reason why the attribution is still closely impossible is because the same means are not available at the international scale. That is why it can be argued that the biggest problem for the attribution issue is the lack of international cooperation.

How to apply the existing international laws? The international strategy that was announced by USA early this year and by UK more or less made the same points. The existing international laws would sufficiently cover the cyberspace while it lacks interpretation and specific ideas to apply them to this new realm.

The networks will always remain vulnerable. When it comes to cyber security, this is even truer than it was ten or fifteen years ago when it comes to cyber security. Why is that? By its nature, networks will remain vulnerable because they have to be connected and they have to use the latest technology, latest software and innovative products. It is against their nature to secure networks, so they will remain vulnerable. What becomes important is the ability to detect and recover from the attack, and to keep the bad guys out of the networks. That is the only solution. Otherwise, technology will not provide a secure network. Craig Mundie, one of the top

3 people in Microsoft, said that to secure an operating system, Microsoft, or other software of course who have operated systems, would have to go back to the drawing board, which is not going to happen.

Cyber offers so much opportunity for both communities, bad and good communities. Hopefully, the good side will have the upper hand. In all conflicts, whether it is political, industrial, social or military, there will be a cyber component, whether it is structure, regional conflict, or a military operation. As the General from Switzerland who talked about net centric operations yesterday said, the air force, the army and the navy, and NATO too, had to integrate their commandant control system and intelligence system so that the coordination would be better and the command and control would be faster. That also means that that net centric infrastructure is more vulnerable to cyber attacks. Whoever takes the upper hand in that net centric infrastructure will have the upper hand in the conflict and that will probably be, as also mentioned by some other speakers, at the beginning of a conflict. It is similar to air superiority. At the beginning of a conflict, if a side takes over the skies then it is almost the end of the story. So, in the net centric infrastructures, if a side is able to achieve the information superiority without firing a single missile and without causing physical damage, it will have the upper hand in the whole campaign.

This is not in place right now, but it is not science fiction either. Probably in five or ten years time that is where we will be.

Humanitarian aspects of cyber warfare

Robin Geiss

Professor of Public International and European Law,
University of Potsdam

Before I start my presentation may I clarify that – contrary to what has just been said – I am not a co-author of the Tallinn Manual but one of many experts involved in the process. And as such I would like to point out that nothing of what I am going to say today should be attributed to the group meeting in Tallinn. In particular, since in Tallinn the starting point of our discussions is the law as it currently stands while today I will try to go a little bit further than that perhaps.

For today's presentation I have been given a rather straightforward task. I have been asked to answer a simple question: What are the humanitarian aspects of cyber warfare? I shall try and answer that question in two parts: First of all, I shall try to assess what kind of “real-world” consequences cyber attacks can cause and how they can be addressed within the framework of international humanitarian law. This part is thus first of all a factual assessment which should be neither too complex nor too challenging from a legal perspective. The second part of my presentation will focus on the question: What is it that makes cyber so different? In other words, what are the specific technological characteristics of the cyber domain? And, considering these peculiarities, what kind of difficulties will we encounter when we try to apply the established legal framework of humanitarian law to this new theatre of war?

Let me first turn to the factual assessment – what are the potential “real-world” humanitarian consequences of military cyber operations? In answering this question, I am not going to discuss whether international humanitarian law can be applied to the cyber domain. Rather, I shall start on the assumption that this is the case because, as far as I can see, there seems to be general agreement that at least the fundamental principles of humanitarian law also apply to this new theatre of war.

What are the humanitarian concerns with respect to military cyber operations? Currently, the vast majority of military cyber operations are

cyber-exploitation-operations clearly below the threshold of an attack in the sense of Article 49 of Additional Protocol I. Even the more visible operations that are colloquially referred to as attacks, i.e. the “attacks” against Estonia, Georgia and Iran did not appear to have caused grave humanitarian consequences. Technically, however, cyber attacks against airport control and other transportation systems, oil pipeline flow systems or dams appear to be possible. Herb Lin in his presentation has just given us some examples. Even more catastrophic scenarios, such as the manipulation of a nuclear power plant or chemical factories, as well as the complete disruption of vital infrastructures cannot be entirely dismissed. Such attacks would most likely have large-scale humanitarian consequences. They could result in significant civilian casualties and damages and clearly they must be a primary concern of any humanitarian lawyer.

How do we treat such scenarios under international humanitarian law (IHL)? In essence there will be no difference whether such consequences are caused by conventional weapons or by cyber means. The same legal principles apply. There is no legal vacuum in cyberspace in times of armed conflict¹. Thus, where cyber operations rise to the level of an attack in the sense of humanitarian law in the context of an armed conflict – and in the horrific scenarios I have just described they clearly would – the principle of proportionality and precautions in attack must be respected. If a party to an armed conflict intends to carry out a cyber attack it is under a legal obligation to conduct a proportionality assessment and to take precautions before launching such an attack. Thus, where the means and methods of cyber warfare produce the same effects in the “real world” as traditional conventional weapons would, I think we encounter no particular legal challenges. States – just as with any military technology – are bound to abide by all of their humanitarian obligations. Thus, the uncontrollable computer virus would be prohibited as an indiscriminate weapon in the same way that the use of a biological virus would be prohibited; whereas a destructive cyber attack that leads to the overheating and destruction of exclusively military cyber installations would raise no particular legal concerns. In the end, there is little difference to a “real world scenario” with traditional, kinetic military means. It all depends on how an attack is designed and in this regard, and this is the point, IHL imposes certain constraints that also apply in cyber space.

That being said, the second part of my presentation focuses on those issues where cyber operations are perhaps so different that the established

1. Cordula Dröge, *No legal vacuum in cyberspace*, online interview, available at: www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm (last visited November 2011).

legal framework may not work out the way it was originally intended. In view of the specific characteristics of cyberspace there is at least a possibility that the application of some traditional rules in the cyber context would off-set the underlying balance of humanitarian concerns and military necessity. There are two issues I would like to focus on: the principle of distinction and the principle of proportionality. There are many more issues – in fact we could go rule by rule – but in view of the twenty minutes that I have been given I shall consider only distinction and proportionality.

First of all, how can you practically distinguish between a military computer and a civilian computer? In reality you cannot tell the difference between a military machine or a civilian machine. Some experts have suggested the marking of military computers in cyberspace but you tell me how likely it is that the military will mark their computers and strategic cyber processes as being military? It's not going to happen. It is simply not realistic that states flag out their most important military cyber assets to the enemy.

But it is not only about how we could distinguish military and civilian cyber assets in practice. Cyber operations also raise a more structural legal issue regarding the traditional definition of military objectives. As everyone is aware the definition of military objectives is to be found in Article 52 of Additional Protocol I. It is accepted as having acquired the status of a customary law rule notwithstanding controversy regarding the interpretation of this definition. The definition tells us – and I am very much simplifying here – that anything that is being used for military purposes becomes a legitimate military objective and thereby a legitimate military target. On this basis any civilian object can theoretically become a military objective. That is the way the law was designed, thereby creating a rather flexible legal standard regarding the definition of military objectives. The thing is, and this is the big difference between the cyber context and traditional warfare, that most civilian objects in the “real-world” are rather unlikely to be turned into any effective military use. This is one aspect in which cyberspace is fundamentally different. Each and every “cyber asset”, every bit of memory capacity or computer power, wherever it resides, has military potential at all times. There simply is no technical difference between a military and a civilian computer. Even a smart-phone suffices to launch a sophisticated cyber attack and every personal computer can be used to create or to send out (fragments of) malicious codes. It follows that in a “cyber war” the established definition of military objectives, albeit it strikes an adequate balance between military needs for flexibility and civilian protection in the real-world, would render basically every “cyber asset” – if not the cyber domain as a whole – a legitimate military objective.

Especially for modern states where many aspects of civilian life heavily

depend on “cyber assets” and a functioning cyber infrastructure this is a worrying conclusion. There is no easy solution for this at all. In theory a narrower definition of military objectives could help to strike a more adequate balance between military necessity and humanitarian considerations for purposes of the cyber domain. Politically, however, such an avenue hardly seems viable. An alternative that arguably better answers to the reciprocal interests of states could be to exclude – either *per se* or under certain conditions – specific systems and cyber assets, such as central servers on which millions of civilian functions rely, from the ambit of legitimate military targets. But in view of the controversy that has traditionally surrounded Article 56 of AP I this may not be a viable option either. A third way could be to allow only certain forms of attack, namely reversible cyber attacks rather than destructive attacks, against such cyber installations that despite qualifying as military objectives nevertheless serve a predominantly civilian function. Again it seems highly unlikely that agreement could be reached on such a solution, which would do away with much of the flexibility that is granted under the law as it currently stands.

With this in mind and in concluding let me turn to the principle of proportionality. The law is rather straightforward about what may be considered relevant “collateral damage”: loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof. There is no indication that the law in this respect has changed in anyway. However, I wonder and I am keenly aware that this is *de lege ferenda* whether this enumeration of legally relevant collateral damages to be considered for a proportionality assessment is still fully up-to-date. After all we have convened this panel here because we all believe that cyberspace has become hugely important, that much of modern life and in fact vital services rely on a functioning cyber infrastructure. Yet, while the destruction of my bicycle would amount to (insignificant but) legally relevant collateral damage (because this would be damage to a civilian object) disrupting cyber services (online-banking) and cyber communications generally for thousands of people, without any physical damage in the “real-world” would not be considered relevant for no civilian objects would have been damaged. In the year 2011 – not long ago there was a G8 summit concerning the internet – I am just not sure whether it is still adequate to treat the disruption of communications as a mere inconvenience that has no legal relevance under international humanitarian law. In this regard I believe it is time to move on and to further develop international humanitarian law. The mere ability to communicate – irrespective of any physical damage – is vital to modern societies. This should also be acknowledged under international humanitarian law.

VI. New technologies: the way ahead

Law, technology and the conduct of hostilities in space

Michel Bourbonnière

Legal Counsel, Department of Justice, Canadian Space Agency,
Longueuil; Member, IIHL

There is a strong and important relation between law (particularly humanitarian law) and technology. At this Institute we have recognized this fact and have acted on addressing it in the teaching curriculum. Indeed, eleven years ago, when we started the Law of Armed Conflict (LOAC) Competition for military academies we discussed the curriculum and the teaching materials. Jointly and in particular with the help of the US Air Force Academy and USMA, we decided to structure a week for the cadets where we would explore the entire spectrum of the use of force and the issues that can come up during a contemporary armed conflict. These issues of concern were not only those of the traditional land, air, naval areas of military operations, but also issues of cyber and space military operations. In establishing the LOAC Competition for military academies and its curriculum, we decided to structure the curriculum to specifically address a generation of new officers that had grown up with computers. Technology is now almost a second nature to cadets. The space and cyber issues were actually very new and difficult issues to deal with for the JOC (Joint Operations Command) leaders as not everyone had practical experience with new technologies in warfare. Seen in this light, the LOAC Competition also allowed practitioners to discuss these new battlegrounds. Thus the LOAC Competition also serves a parallel function allowing military academies to discuss teaching strategies and exchange materials. The Competition is run with four parallel wars, resulting in four JOC centres. The Competition was started eleven years ago, with the participation of eight academies. The success and popularity of this Competition has been phenomenal with rapid growth in participation. We now have approximately 30 academies that participate with great enthusiasm. The cadets are always delighted and thrilled by the experience. The cadets work together in mixed teams of three. The Competition

structure forces the cadets to bridge cultural and linguistic barriers. I would like to invite anyone who has a link with a military academy and/or a civilian university to participate in the Competition. Although initially designed for military cadets, it can also be an excellent opportunity for civilian law students to see how the military process functions on targeting issues. The next edition of this Competition is to be held in the last week of March, 2012. Please feel free to contact the Institute if you are interested in this event for your students.

Law and technology is incredibly pertinent to the conduct of war and the resulting issues can be analysed in a philosophical manner. There are a lot of amazing concepts of technology that can be applied and some authors have noticed and commented that computers can be faster and more ethical than soldiers as computers can “think” faster than humans. Programming computers to function within the legal regime is an interesting concept and programming perhaps fully autonomous computers to respect the laws of war or humanitarian law is an intriguing concept. This is a beautiful dream, but it is perhaps a misleading dream. Law and legal advising is more than just computing. Although, the mathematical paradigm is often the way scientists perceive law. This scientific paradigm yields the impression that law can be easily computed. If this was the case, lawyers would have been long ago replaced by computer programs. The fact that lawyers can express different opinions and different perspectives upon certain issues is in fact what gives lawyers their value. The giving of legal counsel is a question of perspectives. It is important to remember that soldiers are trained, they are not programmed. Soldiers are trained knowing that they are individual, free thinking, sentient beings who will have to react quickly and correctly in unforeseeable complex situations. A fully autonomous robot could never be completely programmed to always react correctly in the Clausewitzian fog of war. There will necessarily always be certain issues and certain things that robots could never do, or be “trained” to do on the battlefield. You can certainly talk about distinction, proportionality and try to calculate it. However, there is a degree of human warmth and compassion that a fully autonomous robot will never have. You can perhaps create robots to destroy things and to break things, but a robot will never win the hearts of the population nor will it win peace. This is done by soldiers and they are the true heroes.

Moreover, law never regulates technology. You have for example, for acceleration due to gravity which expressed mathematically is 9.80665 m/s^2 (32.1740 ft/s^2). This is a law of nature that is expressed in a specific mathematical formula and human law will never change that. Again, this is the law of nature, not the law of men. What the law of men addresses

is always the competing human interests that result from technology. On this point, you have the interest of the civilians, you have the interest of the victims and you have the interest of the soldiers and that of the belligerent states. Used in specific situations, in specific ways, advanced technology and fully autonomous weapons can be good and can bring benefits. However, certain issues remain of concern. For example, if it is possible to have a fully autonomous robotic army, the decision to go to war can be much easier. Right now, the decision to go to war or to go in armed conflict is about sending our sons and daughters into areas of danger. The facility through which armed conflict can possibly occur if the human factor is removed from one side of the equation is one issue that worries me. If the only human sacrifice that remains is removed completely from one side of the equation, the propensity for armed conflict can be increased. On the positive side, the reduction of human risk also referred to as the “body bag factor” could facilitate humanitarian motivated military intervention where human casualties represent an unacceptable political risk for a country. In any case this question deserves much scrutiny.

Space is a specific domain that is permeated with irony. The space age began probably with the V-1 or the V-2 rockets. With the historical flight of Yuri Gagarin began this beautiful dream of endless human space exploration, but there also came perhaps the greatest danger that humankind has ever faced: that of total nuclear warfare and amazing forces of destruction. Yet, space technology has also been developed to help humankind and that is what has been described by Conrad Lorenz and what is known now as the Lorentzian paradox. This philosophical paradox describes a technology that is developed to help humankind, to help evolve and develop our society, but that can also be used to create destruction and suffering. Space technology expresses eloquently this paradox.

Space is an important pipeline. Satellites are the space dimension pipeline of information technology. There are specific treaties that deal with space, namely the Outer Space Treaty within which all countries have agreed that space is to be used for peaceful purposes. Peaceful purposes, however, in not peaceful means. Gulf War One was extremely violent, but it was for peaceful purpose. That is to restore peace. The Outer Space Treaty makes a reference to the applicability of international law and the UN Security system in outer space. Therefore, humanitarian law applies to outer space as the “*lex specialis*” during an international armed conflict in outer space. However, space has specific, physical attributes and changes the application and the calculus of certain traditional and fundamental principles of LOAC, which in a sense makes the use of space more secure.

Theresa Hitchens' presentation about space weapons, earth-to-space, space-to-space weapons was very relevant and her distinction between kinetic, space weapons and directed energy weapons is extremely interesting and extremely valuable. In the calculation, for example of proportionality or of collateral damage, what is interesting in space is that the actor itself while applying force has to take into consideration its own self-interest. If, for example, someone is to do a kinetic destruction of a satellite, there will be space debris and if the space environment itself is harmed, one's own ability to use space is harmed. Thus, the self-interest of the actor is an important variable in the calculus of the damage which is caused in outer space.

When looking at the applicability of humanitarian law to outer space, one sees a cognitive dissidence as to how space is perceived by humanitarian law. One can look at space as a location that could be attacked because it is the ultimate high-ground (AP I Art. 52). Contemporary military doctrine articulates that the ground superiority is contingent upon air superiority and air superiority is itself contingent upon the dominance of the space medium. Yet, space can also be perceived through the rules of humanitarian law as an environment that must be protected (AP I Art. 35). Which one of these interpretations will dominate or will end up being the winner in state practice is impossible to predict. Hopefully, it will be the second option.

Going back again to the philosophical approach of law one can establish three reference points in evaluating a normative structure. As mentioned above, the purpose of a law will always be the regulation of the competing human interest that results from technology. Secondly, the subject of the law remains the ultimate actor who is addressed, namely the human individual or the state itself under international law. Lastly, the goal of the law must remain as a constant, namely the dignity of the subject. It is this triangulation of the law between the three poles that determines the efficiency of the normative structure. If you make laws banning weapons, the law does not affect the weapon itself it affects the ability of the actor to either develop, procure, deploy or use these weapons.

How is this to evolve and what is the future of law regarding these technologies? Well, from an institutional perspective, in the UN there is the Conference on Disarmament (CD). In the Conference on Disarmament, there is a topic called PAROS (Prevention of an Armed Race in Outer Space). PAROS represents a very noble dream and a very useful concept, but it is one which is presently in a political stalemate due to a diplomatic *Zugzwang*. There are fundamentally two positions: one, adopted by the United States, which is refusing to endorse, for various reasons, a

prevention of an arms race in the outer space, and other countries that endorse the proposition of such a treaty. Yet, because of the way that CD functions, namely by consensus, it is presently in a stalemate.

There were two ASAT (Anti-Satellite) tests in the past few years that have become very much of strong interest. One was the Chinese ASAT test that destroyed an aging FY-1C satellite in polar orbit and the other one was not a test, but was actually the destruction of an American satellite (USA-193), by American forces, of a satellite that was re-entering the atmosphere. There are various legal issues that surround both tests. There is just one relevant aspect to the discussion particularly worth underlying: the targeting vector of each of these tests. The Chinese targeting vector was done on the orbital plan and a kinetic ASAT was used. Thus, once the satellite was destroyed, the result was a projection of a large amount of space debris within a certain orbit. This was a relatively low earth orbit approximately 500 miles in altitude. I inject a caveat here, because when talking about space, one must remember there is actually no legal definition of space and that consequently, there is no legal boundary established between airspace and outer space. This being said after the Chinese ASAT test created an important debris field a Canadian satellite, namely the Radarsat 2, had to be manoeuvred several times to avoid collision with the resulting orbiting space debris. As for the American test, I am informed that the targeting vector came from above and hit the satellite downwards, towards the earth thus, projecting the debris field downwards thus minimizing its impact on other space assets. Furthermore the interception occurred at the lowest orbit before the satellite started to tumble in its re-entry so it was still in a predictable orbit. The US interception actually proved that you can use an ASAT weapon in a way that does not cause harmful space debris.

Space warfare is here. It exists. It has already occurred. When two countries go into an armed conflict, the first thing that they try to do is to neutralize the senses of the opposing force, that is, its ability to see, its ability to hear and its ability to speak. Those are all contingent upon space assets. That being said, space war does not necessarily occur in outer space. If the ground control centre of the satellite is attacked, including the principal and the backup station, it will be very difficult to control a satellite afterwards. With a basic SCUD missile on which there is a nuclear weapon it is possible to send this missile up in the lower earth orbit (LEO) and destroy the lower earth orbit and with the resulting electromagnetic pulse affect many satellites and practically render the orbit non-usable. Another example of space warfare, because space warfare is simply the denials of space assets, occurred when Saddam

Hussein had put oil around Bagdad and lit this up and created clouds of smoke. These clouds of smoke in fact created a type of shelter, which prevented optical satellites from imaging. Even if there are radar satellites that can still function at night time or daytime, through smoke or clouds, space warfare remains vulnerable to jammers as the technology that jams a GPS or other communication satellites is widely available and is not a complicated thing to do.

In my view the space environment is more protected during armed conflicts than during peacetime, showing once more its irony, if some debris fields in outer space are created during an armed conflict, many questions have to be taken into account, namely the question of proportionality, the question of one's own self-interest and the question of respecting the rights of neutral states to use and to navigate through space. All these are controlled and regulated through international humanitarian law, but during peacetime, or outside an international armed conflict LOAC does not apply and there is nothing right now, within the corpus of international law that prevents kinetic ASAT tests. So, perhaps, following the logic of the Limited Test Ban Treaty (LTBT), an initial treaty that would ban kinetic ASAT tests could in itself protect space and protect the space environment.

For the use of fully autonomous robots, I question who could be criminally responsible for the use of these robots. Could a computer programmer program these robots so that they function correctly and supposedly in accordance with the laws of armed conflict? If there is one certainty in war, it is that it is impossible to know what is going to happen in war. If one is to program a fully autonomous robot based on past experiences, then, conceptually speaking, one is programming a robot to fight the last war. Is it not a cliché to say that generals always prepare to fight the last war rather than the next one, and is this not generally considered to be an error of strategic importance? Should one of these fully autonomous robots go "stupid" as sometimes happens with smart weapons, there has to be a liability regime which holds the owners of these things responsible. So, perhaps strengthening the liability regime or the responsibility regime would be an option in this connection or, depending on the evolution of the technology involved, even going at some point towards an absolute regime responsibility for those who own and operate these fully autonomous robots. The fundamental issue is necessarily that of accountability and competing human interests. Those who decide to use fully autonomous robots during an international armed conflict, thus avoiding the human costs of life on their side of the calculus should nonetheless remain accountable should there be innocent victims from the

use of these machines, irrespective of the quality of the programming. In other words efficient computer programming should, by itself not be of sufficient legal standing so as to exonerate the owner/operator of a fully autonomous robot from criminal liability. An effective liability regime will go a long way in assuring the correct use of these machines and increase the need for their constant human supervision. A treaty should be the instrument of choice to achieve these goals. In any case a legal duty should also exist to remotely deactivate these machines in a post conflict period. For law to be vibrant it must be pertinent. In order for law to be pertinent the competing human interests must be addressed and, during armed conflict, one of these pivotal human interests remains the human dignity of those who are affected by the conflict.

Law at cyberspeed: answering military cyber operators' legal questions

Gary Brown

Staff Judge Advocate, US Cyber Command, Washington D.C.

The role of the legal advisor to a military operational commander is to provide relevant and accurate advice on military operations in a timely fashion. As much as possible we review operations beforehand, but inevitably situations arise with unique aspects that require another look. The work of our academic colleagues is vital in this regard in that it provides us with the background material on which we form our advance decisions. As military technology has progressed, the speed at which situations evolve has grown ever swifter. Air operations brought us situations changing significantly in minutes. Cyber operations have taken that to incredibly short times – the speed of Internet traffic is measured not in seconds, but rather in milliseconds¹.

The point here is that operational legal advisors have little time for consideration, and have an imperative to answer. In the middle of a military operation, the right answer is never: “I’m not sure”. Modern military commanders rely on legal advice to ensure they comply with international humanitarian law (IHL).

If we date cyber operations from 1982, we’ve been at it for almost 30 years². For all that time, the international legal community has failed to come to consensus on some of the foundational legal issues in cyber operations, such as “what constitutes a use of force in cyber?” and “what kinds of operational cyber activities can civilians engage in without losing their protected status?”. The questions are endlessly fascinating but they have been asked many times. At some point, answers must be forthcoming if the law is to be relevant to cyber operators.

1. See, for example, www.internettrafficreport.com/faq.htm#response.

2. A Russian pipeline explosion in Siberia was reportedly caused by CIA-implanted malware. Bret Stephens, “Long before There Was the Stuxnet Computer Worm There Was the ‘Farewell’ Spy Dossier”, *Asian Wall Street Journal*, 10, Jan. 19, 2010.

In the absence of an established international consensus, military legal advisors are not excused from providing advice. With that in mind, I provide working answers to a few basic questions. It may be that, over time, custom and practice will dictate changes in these answers, but for now, they serve to prevent deliberation constipation.

1. *Where is cyberspace?* By itself, this answer isn't terribly important to operators, but answering it enables answers to other questions that are relevant. On this question, I confess, my answer is a bit ambiguous, because it can be. So, the answer is:

a) *Cyberspace is everywhere.* For almost no cost, anyone can take action anywhere in the world – and do it right now. Computer expertise is no longer required – during the Georgian-Russian hostilities in South Ossetia in 2008, the website stopgeorgia.ru offered software for download that could be used for denial of service operations and other disruptive activity against computer networks in the Republic of Georgia³. Now for €5, one can obtain sophisticated malware and execute extensive cyber mischief through a drop down menu⁴.

Cyberspace provides the backbone for our utilities (electricity, gas, water), communications (Internet, email, telephone service, etc.), emergency services (911, 999, etc.), transportation (air traffic control, railroad switching and routing, traffic lights), logistics (seaport scheduling, trucking deliveries, inventory control), medical care (remotely accessible medical implants, medical records storage, remote access to medical expertise) and more. Controlling home appliances through cyber is becoming even more common. Each of these conveniences presents a vulnerable aspect. However...

b) *Cyberspace is nowhere.* Although the vast majority of Internet infrastructure⁵ is privately owned and the physical parts of it, of course, reside in physical space, those facts are largely irrelevant to cyberspace operations. What makes cyberspace such an incredible engine of commerce, communication and wealth creation is the

3. John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, Aug. 12, 2008, available at www.nytimes.com/2008/08/13/technology/13cyber.html?em.

4. Matt Liebowitz, "How to become a Cyber Criminal for only \$7", *Security News Daily*, Sept. 22, 2011, available at www.securitynewsdaily.com/how-to-be-a-cybercriminal-for-7-1173/.

5. Not everyone considers the Internet and cyberspace to be synonymous, but rather see the Internet as only one method of accessing cyberspace. Some view cyberspace as a reflection of the noosphere, or sphere of human thought. See, for example, Loux, Blantz, Saad *et al.*, *The Synaptic Web*, available at <http://synapticweb.pbworks.com/w/page/8983891/FrontPage> and the *Global Consciousness Project* at www.global-mind.org/.

borderless connection of people around the globe. If nations weren't willing to let the ones and zeros zip across Internet infrastructure that resides in their physical territory, the system wouldn't work. If states choose to assert ownership of equipment they can – by disconnecting it from the larger Internet. Data packets will simply be re-routed, and “unplugged” states will have converted their equipment into an inventory of expensive paperweights. The location of cyberspace is simply more complicated than the location of Internet equipment.

Unlike other forms of communications, Internet communications are broken down near their point of origin (“packetized”). Each packet is sent individually via the most efficient route as determined by sophisticated algorithm to the destination. Near the destination, the packets are reassembled into a whole, which can be delivered in fractions of a second to the addressee. During the journey, each packet may traverse cables, switches, routers and servers located in many countries.⁶ The willingness of nations to allow this free passage of data across its equipment is what makes the Internet work. If this openness ended, so would the Internet as we know it.

2. *What is the extent of cyber sovereignty?* Cyber sovereignty is precisely as much of cyberspace as a nation is able effectively to defend; i.e., not very much. Deputy Secretary of Defense William Lynn reported in July, 2011 that 24,000 files related to DoD projects were stolen from US companies in a *single* intrusion; he estimated the cumulative economic value of data stolen from the US at over \$1 trillion⁷. In short, to experienced operators, whether criminals, “hacktivists” or spies, the computer networks of every nation are essentially an open book. A statement that acting on a nation's computer networks violates its sovereignty is more like a punch line than an assertion of international law. Until there is some evidence that nations and the international community can effectively act to defend national cyberspace, cyber sovereignty is non-existent.

This situation is analogous to the historical development of the limit of national territorial seas. The first recognized distance of a

6. Only about 10% of Internet traffic flows through satellites; the vast majority moves through land and undersea cables. Sarah Kliff, “The Internet is, in fact, a series of tubes”, *Washington Post Ezra Klein's Wonkblog*, Sept. 20, 2011, available at www.washingtonpost.com/blogs/ezra-klein/post/the-internet-is-in-fact-a-series-of-tubes/2011/09/20/gIQALZwfiK_blog.html?wprss=ezra-klein.

7. Deputy Secretary of Defense Lynn's comments during the *DoD Strategy for Operating in Cyberspace* ceremony, Jul. 14, 2011, available at www.defense.gov/speeches/speech.aspx?speechid=1593.

territorial sea was three miles – said to be the distance from which a shore-based cannon could engage ships. In other words, the territorial sea extended only as far as a nation could defend itself. Since then, the distance has grown, but that growth was made possible by the initial agreement among nations to respect the enforceable limit. In cyber today, even if nations all agreed that no activity was lawful “on” servers located in countries without each country’s permission, there would be no way for the community of nations to enforce the standard.

3. *What is a cyber weapon?* The vast majority of cyber operations are carried out without weapons. As the software and communications hardware used to conduct the operations do not constitute weapons, there is no need to conduct a review to see if they might be lawfully employed.

This contrasts with kinetic weapons, which are reviewed to determine if they will cause unnecessary suffering and to ensure they are capable of distinction. This is a relatively straightforward process for traditional munitions such as rifles, ammunition and bombs.

By contrast, cyber operations are often carried out by computer operators, sitting in locations far removed from the target. They send commands using remote access tools – identical to the illegitimate access acquired and used by criminals and spies⁸. These on-net operations just don’t provide us anything that can readily be called a “weapon”. A cyber operator, remotely logged on a network while masquerading as an administrator, can give the network any command the legitimate administrator could. The operation can certainly be reviewed for compliance with international humanitarian law, but there is nothing analogous to a weapon in the equation.

The exception might be physical equipment not based on providing access through the Internet. If devices exist that are able to inject malware directly onto systems, those devices could be considered weapons, although unless they somehow have a kinetic effect, it’s difficult to see how they would require a review for compliance with IHL except as part of an overall operation.

4. *How important is attribution?* Cyber attribution is more difficult but less important than attribution in kinetic operations. In real time, cyber-on-cyber situations, it matters little who is behind the curtain. If a computer

8. Dmitri Alperovitch, “Revealed: Operation Shady RAT, Version 1.1”, *McAfee White Paper*, 2011, available at www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

has been “pwned” and is being used as a launching pad for a cyber attack, how bad is it that it is bricked by the victim as a result?⁹.

In the longer term, attribution to the machine of origin, or even to an individual perpetrator, may be established, but in a situation involving defense of a nation’s financial system or power grid, there would not be time to conduct in-depth forensics before taking action. It is also a complicated, and therefore also expensive, proposition¹⁰. Criminals, hacktivists and other actors all use sophisticated techniques to mask the location of the machine from which they are conducting an operation. And, even when attribution can be inferred, the level of proof is often too low to allow for a public disclosure. As examples, the US Department of Defense has noted major cyber events occurred in 2008 and in 2011, but has not provided attribution of either¹¹. Google’s official statement that China had attempted to penetrate their Gmail system was notable as one of the few public statements of attribution¹².

Attribution is where we can lose sight of the original promise of cyber as a military instrument – it should be seen as a more humane option than more traditional military activities, such as strategic bombing, invading, etc. After all, as much as we love our iPhones, we don’t have a funeral for them when they die. It simply defies logic to require the same level of attribution of a cyber strike as we require for killing people and breaking things.

These answers will continue to evolve over time, but for now they serve to provide a starting point from which military lawyers might develop timely advice to cyber operators.

9. The origin of “pwned” is not universally agreed, but it is most commonly thought to have begun as a computer hacker term for having full access and control over someone else’s computer. See, appropriately, Wikipedia’s entry on the term, as well as Martin Pichlmair, *10 Tales of Appropriation in Video Games*, available at http://publik.tuwien.ac.at/files/pub-inf_4395.pdf.

10. See, for example, David A. Wheeler & Gregory N. Larsen, *Techniques for Cyber Attack Attribution*, Oct. 2003, available at www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859.

11. William J. Lynn III, “Defending a New Domain”, *Foreign Affairs*, Sept./Oct. 2010, available at www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain; remarks on the Department of Defense Cyber Strategy, as delivered by Deputy Secretary of Defense Lynn, National Defense University, Jul. 14, 2011, available at www.defense.gov/speeches/speech.aspx?speechid=1593.

12. David Drummond, “A new approach to China”, *The Official Google Blog*, Jan. 12, 2010, available at <http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>.

Towards a code of conduct for cyber space

Nils Melzer

Research Director, Competence Center for Human Rights,
University of Zürich

I was asked, as part of this concluding panel, to speak on the “way ahead” as far as new technologies and International Humanitarian Law (IHL) are concerned. I will keep my comments brief and simple. In order to make any meaningful statement as to the way forward in any given area, one has to know three things: (1) the problem to be addressed; (2) the environment in which one operates; and (3) the goal or destination of the journey. In following this structure, I will focus on cyber warfare, but you may find that many of my remarks are equally relevant also to other new technologies.

1. The Problem

When analysing the challenge posed to IHL by new weapons technologies, two fundamentally distinct categories of problems should be distinguished: (a) practical or technical problems and (b) legal problems.

(a) Practical or Technical Problems: One category of problems, which has been repeatedly emphasized in the course of this Round Table relates to the practical difficulty of determining the facts of what is actually going on in cyberspace. This includes the initial detection of computer network operations (CNO), i.e. the difficulty of becoming aware that a hostile CNO is being conducted in the first place. Obviously, computer network attacks (CNA), which aim at causing a harmful effect, are more easily detected than computer network exploitation (CNE), which is generally limited to the collection of intelligence data without directly causing any harm. It also includes the difficulties of determining who is the author of a particular CNO and from which location it is being conducted, and estimating its destructive potential both in military and in humanitarian terms.

However, all of these problems are practical or technical, but not legal, in nature and, therefore, can be resolved through practical or technical means only, but not by means of the law. Also, it would be a mistake to believe that these difficulties are entirely new. In the early days of air warfare, hostile airplanes could be detected only once they were near enough to be visible or audible. But then the radar was invented and solved that problem – until the stealth fighter came along. And so the technological development will continue forever. I submit to you that the same will happen in cyberspace. We may not always be able to detect the author of a CNO today, but I have no doubt that technological innovation will surely provide solutions to this practical difficulty much faster than we may anticipate today. What is important, however, is to recognize that the law is designed to resolve legal problems only, not technical ones, and that the persistence of such practical problems cannot, therefore, serve as proof that something is wrong with the law.

(b) Legal Problems: the second categories of problems, the legal ones, are those which we as international lawyers must solve. The focus here is on trying to fit a set of determined facts, within the concepts and provisions of existing law. Very often we will find that, once the factual/technical problem has been resolved, the legal part of the analysis does not pose any particular problem. For example, once the author of a CNO has been identified, the legal attributability of the CNO to a particular State is regulated by the general international law of State responsibility. In case of doubt, the law requires that a particular presumption applies. Only once this exercise leads to unclear answers and the facts in question do not neatly fit under the existing law, we now face a genuine legal problem, for which there are essentially two remedies: First, the meaning of the existing law can be clarified through the methodology of treaty interpretation. This may provide answers to questions such as what constitutes “force” (Art. 2.4 UN Charter) or “attack” (Art. 49 AP I) in cyber space, or what the obligation of combatants to distinguish themselves from the civilian population means in cyber space. Second, where legal interpretation does not provide the answer, and only then, there may actually be a need to further develop the existing law through the creation of new or more precise rules.

Let me emphasize that, in clarifying and developing the law, we should not be afraid of the “high tech” nature of new weapons technologies. We should not believe that just because we do not understand how a cyber attack really works we somehow lack the expertise to regulate such operations for military and humanitarian purposes. After all, we did not hesitate to come up with rules for air and missile warfare, although most of

us lack detailed knowledge of how a jet fighter or missile really functions. Sure, some aspects of our work will need the input of engineers and other technical experts. But what counts for legal regulation is not how a weapon functions, but what its potential military and humanitarian effects are.

2. The Political Environment

Let me now briefly turn to the second determinant aspect of our journey, the political environment in which we find ourselves. As we have heard from various speakers at this Roundtable, there is widespread international awareness today of: (a) the global interdependence and interconnectedness of the international economic, security and political system; (b) the vulnerability of that system particularly to malicious cyber activities; (c) the everyday nuisance, economic and social harm caused by various forms of cyber crime; and (d) the potentially catastrophic humanitarian impact of major cyber conflict. We also seem to have international consensus as to the fact that there is an urgent need for internationally agreed upon standards for acceptable State behavior in cyber space. And last, but not least, there seems to be a marked distrust and divergence of interests between the major “Cyber Powers”, which render traditional treaty negotiations difficult.

3. Way Ahead

Now what does this mean for our “way ahead” on the issue of new weapon technologies and in particular cyber warfare? I agree with previous speakers that, in view of the current political environment we just discussed, there is no potential for the successful negotiation of a multilateral treaty comprehensively addressing and regulating these issues. On the other hand, that same political environment is also marked by the recognition that something needs to be done. But what? Please allow me to put forward a proposal, which may perhaps prove helpful in taking us a step further.

A few years back there was in many ways a similar situation with regard to the dramatically increased activities of private security and military companies (PMSC) in situations of armed conflict. While there was universal consensus that something needed to be done to regulate the activities of PMSC, the disagreement among States on these issues made it impossible for a multilateral treaty to be negotiated on the level of the United Nations. What was successful, however, was a joint initiative by

Switzerland and the ICRC, which led to the adoption by 17 States (now: 36) of the “Montreux Document” in 2008. This document consists of two parts. The first restates existing international legal obligations of States as far as they are relevant for the activities of PMSC. Thus, it does not create new obligations, but identifies the lowest common denominator on which States were able to agree. The second part goes beyond that and consists of a comprehensive compilation of good practices, by which States can implement their legal obligations with regard to the activities of PMSC.

I submit to you that, different as the issues may be in terms of legal substance, there are a number of striking similarities in the surrounding circumstances. First, the issue of cyber conflict is politically delicate. Second, for the time being, States cannot agree on new treaty rules. Third, the entire world agrees that, nevertheless, something must be done to clarify the rules of the game. I, therefore, believe that the unique formula of the Montreux Document, which allows participating States to be conservative as far as the recognition of legal obligations are concerned, while being progressive in recognizing non-binding good practices, may constitute a promising way forward also for the context of cyber conflict. Why not convene a number of key States, including all major Cyber Powers, let them identify their lowest common denominator, such as the basic principles of IHL, and then work our way forward for as long as consensus can be achieved. Beyond that, let the participating States identify a non-binding catalogue of good practices, which shall guide and inform them in their activities in cyberspace. I believe that if we can achieve this, we will have made a great step forward in establishing an international code of conduct for acceptable behavior by States in cyber space.

But when we go about doing so, let us not forget what the original goal of the journey was, is and always must be. It is not about short term political interests, science fiction or unimportant technicalities – but about nothing less than ensuring the rule of law in an entirely new domain of warfare. It is about ensuring a proper balance between the fundamental principles of military necessity and humanity also in cyberspace and, ultimately, about ensuring that those most affected by cyber conflict, whether civilians or combatants, receive the protection they are entitled to not only by law, but also by their very nature as human beings.

Discriminate, precise, proportional

Yedidia Yaari

President and Chief Executive Officer
Rafael Advanced Defense Systems Ltd., Haifa

Today I will try to present what can be achieved in terms of technology in the immediate circle. I will not go in the outer circle like cyber or space. My concern is just to show to what extent it is possible to be more discriminate, more precise and more proportional with the technology as it is now. Probably, the idea that I would like to emphasize is that it is our responsibility to convince the decision-makers that they have to go for stricter constraints on the use of force as today the technology is available and enables it.

I will demonstrate my argument and show the actual development of the technology through specific examples. Some of them are closer to the audience, some are slightly more remote, but they all concern simple soldiers and not too smart weapons. The dilemma is not between dumb soldiers and smart weapons or vice versa, but simply on the right combination of the tools and the training and probably the education and the basic assumptions of what is permissible and what is not.

Let us start with the principle of discrimination. There are three requirements stemming from it: detect the relevant objects, identify who or what it is and discriminate between combatants and civilians. Here I intend civilians in the sense of non combatants. First, let us take the example of a simple operator with the mission of detecting and identifying. There are now sensor devices that can detect moving objects and from something like nine or ten kilometres in the air and distinguish and separate them from inert objects. These sensor devices can also enlarge specific parts of a scene in order to obtain more precision and identify with more certainty the different objects. These are devices that are already operational and when it is necessary to pin point, separate a legitimate separate target from the rest of the pack it is feasible. It is just a matter of creating the infrastructure in terms of both technology and training allowing a good level of data before pulling any trigger.

Another example concerns Italian militaries that, thanks to new technology, were able to detect and recognize an ambush against French militaries in Afghanistan. This is once again in the category of discrimination. The level of precision in discrimination between legitimate targets from illegitimate targets is much more advanced these days. The Italian jet fire is capable of detecting any moving object from a database that was taken half an hour before. One flight gives the first status of things, the state of affairs of a given area, and the next one, which can be immediately after the first flight or much later, will allow the system to detect any changes in the initial status in such a way that if somebody moves a can of Coca Cola ten centimetres from where it was before, the system will pinpoint a change in the status. This is neither cyber nor space, it is a pod attached to existing military equipment that are already used in every day missions.

Then it is necessary to discuss what is intended by being precise. First, there is no more shoot and forget. This is a luxury that no one has any longer. Everybody is responsible for the shot from the moment the aim is defined through the moment the trigger is pulled until the moment the target is hit. That is a full responsibility. Second, a dynamic situational awareness is necessary. The term dynamic indicates that an awareness of the evolution of a situation is needed at all times. This means that a man in the loop is necessary at all times, for every mission. Thus, it is not robotic, there has to be human control on the entire process.

To demonstrate this argument, two examples will be discussed more in detail. The first example is a shot taken from a helicopter where the gunner is given an enemy target. The target is a truck suspected of containing terrorists. The shot is launched from a distance of about six kilometres. The sensor is in the nose of the missile and there is a link that transmits the video from the sensor of the missile to the operator. Therefore, the operator sees for the entire shot exactly what is happening, what is the target and is thus capable of responding when the target is an illegitimate one. Indeed, in this example, during the final seconds of the missile flight, the gunner sees a TV sign on the truck, and instantly aborts mission by driving the missile to the ground. There is no commander, no officer nearby that has to take the decision. It is the decision of the operator. This is feasible in the new type of personal missile that is produced everywhere in the world. In addition, it greatly and precisely answers the three said requirements: a constant man in the loop, a dynamic situational awareness and no more shoot and forget.

Another example of what we mean by precision, again, from a real war scenario. It concerns a target behind which, according to intelligence,

there should be a post of terrorists or, for the sake of neutrality, let us call them enemies. Those enemies are over a hill. Usually, that would call for artillery barrage in order to soften the target and then the infantry would be sent, but not this time. There is no shoot and forget and, in addition, any statistical type of weaponry is avoided because of their inaccuracy. Once again, the sensor is in the nose of the missile, which is launched from the ground from a distance of about seven kilometres. While the missile is shot, something white is detected by the sensor on the field. It is the roof of the building, which is the legitimate target. The sensor sees one building, one target, and then sees a window. Suppose that in that window, in this very moment, there was a girl looking outside, the result would probably be, the same as with the TV. In our example, there is no one, so the missile penetrates inside that window. This illustrates that, given the right intelligence and demanding from the outset that operations are made on that type of intelligence, it will result in something, definitely in the lines and spirit of this conference.

Now, the principle of proportionality, which is softer, will be discussed. What can be done is changing the basic assumptions of design requirement for engineers by asking them to design for the minimal required effect instead of maximizing destruction. It makes no sense to maximize destruction or something that is anyway inert and not contributing in warfare in any sense. It is necessary to be more precise and more proportional in order to be more efficient in terms of investments, energy and resources. Efficiency wise and given that precision is already available, designing for the minimal required effect appears the right and logical goal for the engineers. The last option I would like to underline is the fragment-free ones. It is feasible. We already have munitions that can be almost totally fragment free. There are composites and materials that do not spread out as fragments and the only impact is the one of the explosive itself.

What has been presented here is a line of thinking in the technological mind-set that insists on and effectively implements the existing constraints and that does not tolerate mass destruction options so there is no statistical weaponry, nor are there options of producing something that is not precise, discriminatory and proportional. Certainly, collateral damage, under these assumptions, is not a necessary evil. It will happen, but it is possible to reduce it dramatically, because the technology to do so is there.

Concluding remarks

Philip Spoerri

Director of International Law and Cooperation, ICRC, Geneva; Member, IHL

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 cyberspace.

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.

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's 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 cyberspace 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 about – this was the credo of many speakers here in Sanremo. 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.

Concluding remarks

Wolff Heintschel von Heinegg

Head of the Faculty of Jurisprudence, European University of Viadrina, Frankfurt (Oder); Member, IIHL

In its 1996 Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, the International Court of Justice held that “it cannot be concluded [...] that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons. Such a conclusion would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future”.

This part of the Opinion has often been referred to, sometimes even abused, when the applicability of the law of armed conflict/international humanitarian law to new weapon technologies was at stake. Indeed, the passage from the Advisory Opinion has the potential of comforting those who have an unpleasant gut feeling whenever new weapons technologies have been introduced or reported about. I cannot escape the impression that some of the discussions we had during the last two and a half days were guided by such a gut feeling rather than by a sober legal and factual analysis.

Of course, new weapons technologies are all too often surrounded by secrecy that is unnecessary and counter-productive. That secrecy has led many to develop a picture of new weapon technologies that is shaped by the media – and sometimes even by Hollywood. It is incontestable that the media have a considerable impact on the debate on the legality of the use of modern weapon technologies. For instance, the use of drones is a most attractive subject to all those reporting on military operations – irrespective of whether they pursue a certain agenda or not. Drones are often described as autonomous killing machines that, once the target has been identified, attack without regard to the collateral damage that may be inflicted upon civilians and civilian objects. What is sometimes forgotten

in the various reports on an allegedly unlawful use of drones is that the use of systems that operate on the basis of certain pre-set parameters is not necessarily a new phenomenon of warfare. For instance, in naval warfare the use of mines responding to certain signatures – acoustic, electromagnetic or pressure – is quite common and legally uncontested. Seemingly, the sinking of ships is less exciting and attractive to the media than the downing of an aircraft or the killing of a Taliban fighter (performing a “continuous combat function” and thus constituting a lawful target) in Pakistan. The commotion about the use of drones clouds the very fact that such unmanned aerial vehicles are nothing but platforms. They qualify as military aircraft if they comply with the criteria of the generally recognized definition. While they may carry and deliver weapons, they are not weapons. So why, one may ask, is the discussion about the use of drones so intense? Probably the right answer is that they can cover long distances and deliver their ordnance with a “man in the loop” or “man on the loop” situated at a far distance from the target area.

It is important to emphasize that, according to the position taken here, the International Court of Justice is absolutely right when applying the existing international humanitarian law to new weapon technologies. There can be no doubt that the basic principles of that law apply irrespective of the novelty of the methods and means employed. Therefore, all the speakers who have taken the view that the existing international humanitarian law is sufficiently developed and flexible to cope with all the issues surrounding the use of unmanned systems, i.e. drones and robots, have rightly rejected claims aiming at the adoption of new treaty law. Nevertheless, the applicability of the existing international humanitarian law to new and increasingly autonomous systems should not mislead us to believing that there is no necessity for a thorough and sober legal analysis. The legal issues surrounding the introduction of new technologies are not solved by mere reference to the principal applicability of international humanitarian law and to the obligation to perform a review of new methods and means of warfare. For instance, compliance with the principle of distinction already is a most demanding task when conventional methods and means are used. The ensuing technological challenges for semi-autonomous and autonomous systems are obvious. Similar considerations apply with regard to the obligation to take all feasible precautions.

The legal analysis must be conducted in a sober manner. Especially, it may not be guided by considerations lying beyond international humanitarian law. Otherwise, the persuasiveness and operability of international humanitarian law would be extremely jeopardized. For

instance, the use of drones is all too often analysed by reference to an arbitrary combination of *jus in bello* and *jus ad bellum*. While there should be agreement on the continuing distinction between the two bodies of law the discussion on “targeted killings” or “extrajudicial killings”, e.g. by drones in Pakistan, very often ignores that distinction. In the course of an armed conflict – international or non-international in character – the legal issues at stake are those of international humanitarian law. However, not every operation that is rightly or wrongly characterized as “targeted killing” is to be evaluated in the light of the *jus in bello* but rather of the *jus ad bellum*. Very often it is an issue of whether that form of “extraterritorial law enforcement” is justified in the light of the prohibition of the use of force under Article 2 (4) of the UN Charter. The legality of the use of the platform, of the weapon used, of the target and of the “collateral damage” under international humanitarian law is to be established independently from the *jus ad bellum* issue of “extraterritorial law enforcement”.

Seemingly, cyber operations are even more difficult to deal with under the existing international humanitarian law. For many, cyberspace constitutes the “fifth dimension of warfare” and it is thus excluded from the scope of applicability of the existing law. Moreover, there are but a few specialists who fully comprehend the nature of cyberspace and the capabilities of actors – State or non-State – in the hostile use of cyberspace and cyber means. It is a common feature that a lack of understanding if accompanied by hysterical media reports or governmental statements increases scepticism if not fear of a new technology and the belief that the existing law is not apt to cope with the issues involved. However, as rightly stated by Nils Melzer, applying existing international humanitarian law to new methods and means of warfare, including cyber operations, does not presuppose that we understand every single technical detail. Who among the international lawyers present here would claim to fully comprehend how a submarine or a military aircraft works? Still, nobody would deny any of those international lawyers to present a legal analysis of the use of submarines and military aircraft under international humanitarian law.

In concluding, a short remark on space warfare seems to be appropriate although the military use of outer space has not been a prominent subject. Michel Bourbonnière has drawn our attention to the international instruments and treaties that are of relevance in the context of what may be labelled “space warfare”. It is important to note that warfare in outer space or via outer space is not a matter of some distant future but that it is a reality already today. Unfortunately, international space lawyers are not always aware of international humanitarian law. But even if they are,

they are not necessarily sufficiently knowledgeable in that field. It is highly important that those working in the area of international humanitarian law also take into consideration outer space. “Space warfare” is not a matter exclusively relevant for superpowers’ warfare, e.g. between the US and China. Many States have assets in outer space that are used for military purposes. Hence, it is highly probable that an armed conflict will not be limited to the known three dimensions but that it will also be conducted in the fourth dimension of outer space. While it may seem odd to some, it is far from clear whether and to what extent international humanitarian law would be applicable to the conduct of hostilities in outer space.

It is, therefore, important and would be well in line with the aims pursued by the International Institute of Humanitarian Law and the International Committee of the Red Cross that we all do not too easily capitulate *vis-à-vis* modern and technologically most complex methods and means of warfare but that we analyse and apply the existing international humanitarian law in a sober manner with a view to arriving at operable solutions. Political and other extra-legal considerations, though important to understand, should not have an impact on that most important undertaking.

Acronyms

AI	Artificial Intelligence
AMW	Air and Missile Warfare
API	Additional Protocol I to the 1949 Geneva Conventions
ASAT	Anti-satellite
ATM	Automated Teller Machine
CCCPA	Cairo Regional Center for Training on Conflict Resolution and Peacekeeping in Africa
CCW	Convention on Prohibition or Restriction on the Use of Certain Conventional Weapons
CCWC	Prohibition or Restriction on the Use of Certain Conventional Weapons Convention
CD	Conference on Disarmament
CDMA	Cyber Defense Management Authority
CIA	Central Intelligence Agency
CICR	Comité International de la Croix-Rouge
CNA	Computer Network Attacks
CNAD	Conference of National Armament Directors
CNE	Computer Network Exploitation
CNO	Computer Network Operations
CS	2-chlorobenzalmalonitrile (defining component of tear gas)
DARPA	Defense Advanced Research Projects Agency
DCDC	Development, Concepts and Doctrine Centre
DCI	Defense Capabilities Initiative
DMZ	De-militarized zones
DNA	Deoxyribonucleic acid (gene)
DOD	Department of Defense
ETAP	European Technology Acquisition Programme
EU	European Union
EU/LOI	European Union/Letter of Intent
G8	Group of Eight

GMLRS	Guided Multiple Launch Rocket System
GPS	Global Positioning Systems
HQ	Headquarters
HTV-2	Hypersonic Test Vehicle 2
HUMINT	Human Intelligence
IAF	Israeli Air Force
ICBM	Intercontinental Ballistic Missile
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
ICT4Peace	Information and Communication Technology for Peace
IDF	Israel Defense Force
IDP	Internally Displaced Person
IHL	International Humanitarian Law
IIHL	International Institute of Humanitarian Law
IMPACT	International Multilateral Partnership Against Cyber Threats
IOM	International Organization for Migration
ISR	Intelligence, Surveillance and Reconnaissance
IT	Information Technology
ITU	International Telecommunication Union
JAG	Judge Advocate General
JOC	Joint Operations Command
JOCS	Joint Operational Command Centers
LED	Light-Emitting Diode
LEO	Lower Earth Orbit
LOAC	Law of Armed Conflict
LOI-ETAP	Letter of Intent-European Technology Acquisition Programme
LTBT	Limited Test Ban Treaty
LTTE	Liberation Tigers of Tamil Eelam
MAD	Mutual Assured Destruction
MLRS	Multiple Launch Rocket System
MOD	Ministry of Defence
NAD	National Armaments Directorate
NATO	North Atlantic Treaty Organisation
NATO RTO	North Atlantic Treaty Organisation's Research & Technology Organisation
NDPP	NATO Defence Planning Process
NEO	Network Enabled Operations
NGO	Non-Governmental Organisation
NLCS	Non-Lethal Capabilities
NLWS	Non-Lethal Weapons
OCCAR	Organisation Conjointe de Coopération en matière d'Armement
OIM	Organisation internationale pour les migrations
PAROS	Prevention of an Arms Race in Outer Space
PMSC	Private Military Security Companies

R2P	Responsibility to Protect
R&D	Research and Development
RMA	Revolution in Military Affairs
ROE	Rules of Engagement
SCUD	Short-range nuclear capable missile
SLA	Sri Lankan Armed Forces
START	Strategic Arms Reduction Treaty
TV	Television
UA	Unmanned Aircraft
UAV	Unmanned Aerial Vehicle
UCAV	Unmanned Combat Aerial Vehicle
UCV	Unmanned Combat Vehicle
UK	United Kingdom
UN	United Nations
UNEP	United Nations Environment Programme
UNHCR	United Nations High Commissioner for Refugees
UNITAR	United Nations Institute for Training and Research
UNOSAT	United Nations Operations Satellite Applications Programme
UNSC	United Nations Security Council
UNSMIL	United Nations Support Mission in Libya
US	United States
USA	United States of America
USAF	United States Air Force
USMA	United States Military Academy
WW I	World War I
WW II	World War II

