The contemporary use of –and possible limits for– artificial intelligence in warfare: a military perspective

Sean MOORE
Assistant Head, Legal – Development, Concepts and Doctrine Centre at the Ministry of Defence, United Kingdom

Thank you for the very kind invitation to take part in this 42nd Round Table, co-sponsored by the International Institute and the ICRC. It is a genuine honour to be amongst such distinguished and knowledgeable speakers. And it a real pleasure to be back in San Remo. It is far more years than I care to remember since I was a newly qualified naval lawyer getting my first taste if IHL as a student on one of the Institution’s courses.

A bit about DCDC

Before I attempt to address the question that I have been given: the contemporary use of – and possible limits for – artificial intelligence in warfare: a military perspective, it might be helpful if I explain a little about what DCDC or, to give it its full title, the UK’s Development, Concepts and Doctrine Centre does, and how the law (not just IHL) is at the heart of our thinking.
Bringing together Army, Navy, Air Force personnel, as well as Civil Servants and colleagues from many partner nations, DCDC’s outputs and responsibilities include: the Strategic Trends Programme which provides the long term strategic context for policy makers (and if you are interested in our perspective on the possible broader societal impacts of AI, do please read Global Strategic Trends 6); Concepts, which outline how our armed forces and defence may operate in the future; and Doctrine, which provides guidance for commanders based on best practice and operational experience. The work of DCDC underpins MOD strategic and joint force development.

As well as contributing to all of DCDC’s outputs, my small legal team is responsible for the UK’s Joint Manual on the Law of Armed Conflict as well as our guidance and instruction on the treatment of Captured Persons. We also supervise the delivery of IHL training across the Services. And, particularly relevant to this Roundtable’s discussions, we discharge the UK’s responsibilities under Article 36 of AP1 by conducting legal reviews into all new weapons, means and methods of warfare (and I will say a little more about that later) and a member of my team is one of the UK’s Group of Government Experts delegation in Geneva looking at Lethal Autonomous Weapons Systems.

**Human Machine Teaming rather than AI or Autonomy**

I’d also like to say something about terminology and the deliberate choice of the UK to refer not so much to AI but to Human-Machine Teaming.

Much of what I will talk about today is based on a Joint Concept Note DCDC published last year: Human-Machine Teaming. That choice of words was deliberate. There is, or can be, a tendency to become fixated on the technology around AI, particularly as, if you are not steeped in AI coding, it can seem mysterious and potentially omnipotent. But it is not the technology behind AI that is at the core of the legal and ethical issues, but how we chose to use it.

The developing nature of the technologies in this field has created an array of terms and terminology which are often used interchangeably or differently by various commentators. Drawing distinct boundaries between those terms can often prove difficult, if not impossible. We are seeing some of the practical impact of this complexity in the LAWS GGE discussions under the CCW Convention in Geneva. Those of you who have been following those discussions know that the superficially simple task of
agreeing some common definitions has proved a significant challenge in attempts to come up with a framework for the governance of such systems.

And, for clarity, it might be worth me making clear that the UK government’s public ally stated position is that we do not operate and do not plan to develop any lethal autonomous weapons systems.

It is the joining up of humans and machines that is where the contemporary debate about the use of AI is, at least in governments and the military. We are – not yet – in the world of advanced general AI that some like Elon Musk worry about; where human beings become just the biological ‘boot-loaders’ for a future super-intelligent artificial form of life. And we are not yet in an era where autonomous killer robots go rogue and decide that human beings are an unnecessary inconvenience.

Throughout history, new technologies have been a driver of military adaptation and advantage. Whether moving from sail to steam, horses to tanks, or the introduction and exploitation of the aeroplane or radio, the results have often been transformative.

When it has been transformative, strategy, tactics and technology have often evolved symbiotically; invariably when people figure out how best to exploit the full potential of the emerging combination of technologies.

Robotics, and AI, machine learning, big data, and, in due course, quantum computing and quantum sensing, offer the potential for another inflexion point in delivering military transformation and advantage. However, machines do not yet perform as well as a human brain. So, realising this potential will depend on understanding the relative strengths of humans and machines, and how they best function in combination to outperform an opponent. Developing the right blend of human-machine teams – the effective integration of humans and machines into our war fighting systems – is the key; and we should not forget that we are in a race with our adversaries to unlock this advantage. The clock is ticking, as new technology capabilities accelerate.

Contemporary use of AI in warfare

The array of potential forms taken by remote and autonomous AI enabled systems, and consequently how they interact in human-machine teams, is extremely varied. In size and complexity, they could range from a future AI and robotically-enabled aircraft carrier retrofit, to a single, disposable nano-unmanned aerial vehicle. We typically think of these systems as physical robotic systems in the battlespace, however, applying AI particularly for
command and control functions and cyber operations will be increasingly common and important.

Because of the ubiquitous nature of the dual-use technologies of AI and robotics, the impacts on conflict are a matter of when, not if. The effects of these technologies on economics, conflict and society are likely to be increasingly profound and, in the long term, offer new opportunities for strategic overmatch and operational advantage. Harnessing AI will, potentially, give us: increased situational awareness; lighter physical and cognitive loads; sustainment with increased anticipation and efficiency; increased force protection; and, ultimately, superior manoeuvre options in and across all domains. The greatest advantages the confluence of artificial intelligence and robotics development will allow are:

- the ability to scale physical mass and presence on the battlefield independent of the numbers and locations of human combatants;
- extending the reach and persistence of our intelligence, surveillance and reconnaissance (ISR) and weapon systems; and
- information advantage for understanding, decision-making, tempo of activity and assessment.

Command and Control

The use of automation offers opportunities to better exploit information to improve understanding, decision-making and tempo. It will also enable smaller headquarters and more agile command and control. Current UK command systems remain based on significant numbers of staff in static locations with large installed information technology systems. Current configurations are rigid, vulnerable to attack and expensive to reconfigure or redeploy. The move from paper-based to electronic-based workflows has added information awareness and data volume, but at the expense of reduced mobility or structural flexibility. In addition, future intelligence, surveillance, target acquisition and reconnaissance systems will generate much larger volumes of real-time data which will be impossible to process without automated support. Data fusion, automated analysis support and visualisation technologies will be essential to achieving manageable cognitive loads, not just for commanders and staff, but also within individual platforms – warships, tanks aircraft and, eventually, for individual soldiers, sailors and airmen.
Cyber

The application of AI and automation to cyber systems is the most immediate arena for evolution and advantage. The cyber domain’s intrinsically codified nature, the volume of data, and the ability to connect the most powerful hardware and algorithms with few constraints of bandwidth, power access, or limits on speed and repeatability of actions creates an environment where AI can rapidly evolve and optimise to their assigned tasks.

We must consider that the evolving cyber domain will be a complex ecosystem containing billions of competing AI agents. In the civil sector alone, before any combatant AI systems engage, there will be intelligent agents competing over: cyber security; finance; media influence; virtual currency mining; advertising; social media influence; pornography; and every other form of web-based interaction. Furthermore, the Internet of things is dissolving boundaries between the online and physical world. Any deployed cyber system will be exposed to, and become part of, this wider ecosystem; an ecosystem that will also be increasingly indivisible from civil critical national infrastructure.

Remote and Automated platforms

The confluence of AI and robotics development will allow us to scale physical mass and battlefield points of presence increasingly independently of numbers and locations of human combatants. This is similar to the way the Internet has enabled access to information and projection of influence at scale and across the globe by individuals in the virtual domain. Cheap and relatively simple systems are already altering the economics of warfare; an area where the NATO has enjoyed a technological-economic advantage since the 1980’s. In March 2017, the US reported that an ally had used a $3 million Patriot missile against a quadcopter that cost $200 from Amazon. Houthi fighters in Yemen, have employed low-cost drones to disable Patriot missile systems in Saudi Arabia. Future options, such as pilot tunnelling, where defensive systems are overwhelmed by employing massed cheap systems, are increasingly viable. Understanding what this means for the way we fight and force development will be significant.

Novel combinations of human-machine teaming will offer a range of new capabilities. They will present opportunities to augment human teams and manned platforms and even create massed effect, such as swarms.
Networked mass – large numbers of interconnected sensors and soldiers, vehicles, ships and aircraft – contribute to resilient ISR networks, understanding and enable manoeuvre. Cheap, smart systems can provide resilience by absorbing casualties on a scale that will not be viable, or desirable, using a solely manned force; they will also be used to overwhelm an opponent’s defences.

You will have noticed that, so far, I have talked very much at the conceptual level of what AI and autonomy can do. But the reality is that we are already beyond the conceptual stage.

In 2016, the Royal Navy, working with industry and other partners hosted Unmanned Warrior. In the testing environment of the Scottish coast and waters, for two weeks, over forty organisations demonstrated more than 50 different unmanned and autonomous air, surface and sub-surface systems.

The Fusion system onboard the F35 aircraft, in operational service today, relies on a high degree of AI in its fusion of remote and onboard sensors. Similarly, the combat information system being developed for the Type 26 ASW frigate will rely heavily on AI in its operation. The Brimstone missile has a long range, seek and destroy mode for when targets are not visible. And close range (and not so close range) naval missile systems, such as SeaCeptor, have the ability to engage targets automatically.

Possible limits

So, having outlined some of the uses of AI in warfare, I now need to highlight the possible limitations on those uses.

Before I do so, I want to offer a personal opinion about the role of law as a limiting factor. Clearly for those of us who are lawyers, the law, and particularly IHL is probably the first source of constraint that we instinctively turn to. And, of course, we recognise that law has a normative function – hence the hotly contested debates taking place in the GGE in Geneva, not to mention similar discussions that ended in 2016 over cyber activities.

But the law is, in the short term, not, I believe, likely to be the most significant constraint. Societal, cultural and public opinion will have far more impact on the development of these systems, at least in democratic societies and at least until the acceptance of these technologies in everyday life becomes widespread. Most of us will be familiar with Google’s ending of its relationship with the US DOD after its employees objected to being involved in the business of war. And it is public opinion more than law, that
lead the UK to make public its no development of lethal autonomous weapons policy.

Added to public opinion, must be a healthy degree of scepticism over the technology itself. Any of us who have served in uniform will know that even the most expensively procured piece of equipment rarely stands up to the rigours of military life for long. And often fails at exactly the wrong moment. Never underestimate the ability of the ordinary soldier, sailor, airman or marine to break things [just ask the British Army how many Watchkeeper drones they have lost]. And that is without the interference, spoofing, jamming or deception of our adversaries. And, whilst I would be the first to acknowledge the impressive speed of development of AI, it still remains fragile. So it would be a foolhardy government that bet the farm on AI.

So, with that caveat, I will mention a few of the legal issues that we as military lawyers are wrestling with as we look at AI and warfare. And as operational lawyers, I should say that IHL is only one field of law that governs the conduct of military activity. Whilst IHL remains central, the modern military lawyer needs to be able to advise his or her commander on a range of legal issues, from IHL to Human Rights law, domestic and international criminal law to data protection.

**Article 36**

Central to the UK’s position in Geneva has been that, whilst I’m theory turning the battlefield over to killer robots might be an attractive notion to science fiction writers, doing so will not relieve States of their obligations under IHL. And, like any technology deployed in warfare, that must be capable of being used in compliance with our international obligations: whether it is a dumb bomb or a smart robot.

As I said in my introduction, it is my team at DCDC that conducts Article 36 reviews on behalf of the UK. And in doing so, we must ask ourselves can this weapon be used in compliance with international humanitarian law. If the answer is no, we do not pass the system.

I won’t repeat what both Professor Dinstein and Professor Nasu said yesterday about discrimination and superfluous injury or unnecessary suffering. But these key principles are at the core of the Article 36 process. So, when looking at a future autonomous weapon system, we would have to direct ourselves the the very heart of what drives the fear against such weapons. Put simply, an autonomous weapons system that was incapable of being used in a proportionate and distinctive way, or a weapon system that
risked causing unnecessary suffering or superfluous injury would not get near the battlefield.

It is true however that the sophistication of new weapons, particularly highly automated ones, with sophisticated algorithms, incorporating machine learning, does pose new problems for those of us conducting such reviews. But those problems are not insurmountable.

The F35 aircraft is by no means a lethal autonomous weapon system. But it does possess a high degree of autonomy, and the sophistication of its combat system that fuses together data from a range of onboard and off board sensors is beyond anything previously seen. Therefore whilst it is the pilot the makes the decision to fire a particular weapon, in reviewing the aircraft, we had to make sure that he was not simply a rubber stamp to a decision that had in fact been presented to him by a machine. We did this in the way we would any weapon, by looking at the evidence of trials and analysis by systems experts. Conceptually the approach was no different even though in practice the volume of data was far in excess of anything we had previously done.

Article 82

Notwithstanding what I have said about the importance of Article 36, I do think that the nature of machine learning based systems, with increasing levels of autonomy mean that the traditional boundary between the obligations under Article 36, i.e. before a weapons is deployed, and Article 82, the duty to provide legal advice during operations will be come blurred. As systems become capable of operating independently for longer periods and capable of self-programming and adapting, the need to monitor these systems and provide legal advice to the commander will remain. Whether through supervisions by humans or by programming in ‘check if in doubt’ protocols into the systems, will mean that the need for legal advice will become ever more valuable.

IHL Programming

Whilst I fully agree with what Professor Dinstein said about being a long way off from machines that make proportionality decisions, we are already able to programme certain ROE parameters into some systems, do not engage certain IFF responses for example.
A point that Professor Dinstein alluded to yesterday is worth drawing out. Autonomous weapons systems could, if programmed properly be more compliant with IHL. A low cost, disposable weapon systems does not need to be taught the virtues of courageous restraint. It could be programmed not to open fire if there is any doubt as to the legitimacy of the target. Any reasonable commander would be quite content to see a cheap drone destroyed by the enemy rather than cause incessant civilian casualties in a way that they would not for any man or woman under their command.

I said a moment ago that operational lawyers have to think broader than IHL to do their job, so let me conclude by pointing out some of the other aspects of law that can and will limit the deployment of AI systems.

Status – there is a significant debate underway within the naval law community over the status of autonomous vessels. Are they warships with the right to engage in attack, or are they auxiliaries, or are they merely weapons systems. The reality is that they will be a mixture of all three. But uncertainties over status does limit – in the short term – the development of such systems.

As we heard yesterday from Professor Gaggioli, human rights law is playing an increasing role in some armed conflicts. And, in the sorts of quasi-NIAC conflicts we may be facing, where the threshold of IHL applicability is sometimes blurred, and our adversaries are willing to use a range of activities of varying legitimacy to achieve their ends, then human rights concepts such as privacy and the right to life are, in some circumstances, relevant considerations.

More prosaically, we should not forget that these systems are designed by engineers, and if there is one group of people who love rules and process more than lawyers it is engineers, so whilst not necessarily hard law, we must not underestimate the impact of regulatory standards and basic health and safety processes in ensuring that unpredictable systems are not released into the wild.

And as a concluding remark, I could not agree more with Professor Venturini when she said yesterday that training is the key. Even more than law, educating our people in the merits and the limitations of these systems is essential. That does not mean that we need to create a generation of computer programmers. For thousands of years we have lethal autonomous weapons systems, they just happen to be made out of flesh and blood.

Thank you for your time.