

REPORTS AND DOCUMENTS

Emerging military technologies applied to urban warfare

ICRC, Programme on the Regulation of Emerging Military Technologies, Asia Pacific Centre for Military Law, 21–22 March 2018*

IHL symposium report

: : : : : :

Executive summary

The roundtable on “Emerging Military Technologies Applied to Urban Warfare” brought together governmental, military and academic experts from various disciplines, including law, ethics, political science, philosophy, engineering and strategic studies. Over two days, experts from across Australia¹ considered three areas of emerging technology and their intersection with urban warfare: cyber-capabilities, new robotics and autonomous weapons, and human modification technologies. In the final session, the roundtable discussed the influence of new technologies on military and strategic decision-making processes, with a focus on the implications in urban environments.

* This report is a summary of an IHL symposium and does not necessarily represent the views of the ICRC, the Program on the Regulation of Emerging Military Technologies, or the Asia Pacific Centre for Military Law. Special thanks to Emily Defina for her work in preparing this report.

Several themes recurred in the discussions. These included:

- the particular vulnerabilities of the urban environment and its civilian population to the direct and indirect impacts of armed conflicts;
- calls for standard, workable definitions to promote cross-discipline understanding and to inform public debate more generally;
- agreement around the sufficiency of extant law but recognition of the challenges in applying it to new technologies and ensuring compliance;
- the need to look beyond the strictly legal paradigm and incorporate ethical, policy and strategic considerations into the approach to new military technologies;
- the importance of grounding legal and academic discourse in the technical reality and the operational context;
- the value of receptivity to positive uses of new technologies and the risk of inhibiting such developments through hasty blanket prohibitions;
- the possible requirement to deploy emerging technology where it might improve compliance with international humanitarian law (IHL) and humanitarian outcomes; and
- the benefits of a multidisciplinary approach in terms of sharing complementary expertise and providing insight into State practice.

* * *

Introduction

The IHL roundtable on “Emerging Military Technologies Applied to Urban Warfare”, co-hosted by the International Committee of the Red Cross (ICRC), the Program on the Regulation of Emerging Military Technologies, and the Asia Pacific Centre for Military Law, was held at Melbourne University Law School on 21 and 22 March 2018. The roundtable, which took place in the context of the ICRC’s 2017–18 conference cycle on “War in Cities”, gathered governmental, military and academic experts from various disciplines, including law, ethics, political science, philosophy, engineering and strategic studies, to discuss the legal and ethical issues raised by new military technologies, with a focus on their impact in urban environments.

Given the roundtable’s focus on urban warfare, discussions often emphasized the unique vulnerabilities presented by the complex and fragile urban

1 Asia Pacific Centre for Military Law: Professor Alison Duxbury, Sqn Ldr Anthony Erman, Col. Arun Lambert, Ms Grace Corbiau, Dr Robert Mathews. Australian Defence College: Dr Michael Evans. Australian National University: Associate Professor David Letts, Dr Adam Henschke. Australian Red Cross: Ms Isabel Robinson, Ms Kylie Leach. Griffith University: Dr Samuli Haataja. ICRC: Mr Leonard Blazeby, Ms Ellen Policinski, Ms Georgia Hinds, Ms Emily Defina. University of Melbourne: Professor Tim McCormack, Dr Sulette Dreyfus, Dr Tim McFarland, Ms Kobi Leins, Ms Natalia Jevglevskaia, Mr Simon McKenzie. University of New South Wales: Dr Deane Peter-Baker, Dr Jai Galliot. University of Queensland: Dr Rain Liivoja. University of Tasmania: Ms Natalie Nunn. Brigham Young University: Dr Eric Talbot Jensen. With thanks to the governmental and military experts who participated under Chatham House rules.

environment, especially with regard to the difficulty in estimating the reverberating impacts of attacks. In addition, there were several other themes that repeatedly surfaced during the sessions and generated interesting questions for further consideration.

Definitions were discussed in each session, with participants noting competing nascent categorizations of new technologies, which potentially impact the development or interpretation of legal regulation. Participants considered that it could be beneficial to establish some common vocabulary between disciplines; it was observed that disparate terminology impedes the development of cross-disciplinary understanding and poses an issue for messaging and communication between government, the military and civil society.

Existing legal norms were seen as a sufficient framework for regulating new technologies, although further clarification and development of the law may be needed to address certain challenges. Experts stressed the need to clarify the application of current norms to specific situations and technologies, and to work to strengthen compliance. Participants noted that IHL was developed to encompass innovations in warfighting and that its principles continue to be fundamentally relevant – for example, by subjecting new weapons to Article 36 review and regulating a weapon's effects rather than its form. The practical and political obstacles to negotiating new international treaties were considered to provide further impetus to rely upon the current framework.

There was widespread agreement that although the law is the crucial starting point, once a practice is deemed lawful it should nonetheless continue to be interrogated in light of other policy considerations. Ethical issues may be of equal or greater relevance than legal ones; indeed, through reference to the Martens Clause, ethics may influence the interpretation of law or provide a source of law itself.

It was emphasized that the conversation on new military technology needs to be grounded in reality rather than in imagined developments far in the future that may not come to pass. Lawyers and academics must have an understanding of the technical capabilities and potential of the relevant technology and its intended operational use. At the same time, whilst being mindful of these parameters, discourse should not be restricted to the status quo; there must be an attempt to look to the future and plan for contingencies in order to avoid a humanitarian catastrophe resulting from a failure to consider the possible effects of emerging technology.

Participants often acknowledged the potential for positive uses of new technologies in urban environments. Examples included humanitarian uses for technologies, such as aid delivery and unmanned evacuation vehicles, and a reduction in casualties (both combatant and civilian) through minimized troop contact and precision targeting. Several participants expressed concern that pre-emptive blanket prohibitions of new technologies might inadvertently restrict the development of these positive applications.

Some participants raised the thought-provoking assertion that parties with access to certain technologies might be considered to have an obligation to deploy

that technology where it represents the most humane and IHL-compliant option. This was posited as a moral obligation which might also have some legal basis in the context of the restriction on choice of means and methods of warfare for those States party to Additional Protocol I (AP I).²

Lastly, the merits of the multidisciplinary approach recurred throughout discussions as a path towards strengthening the response to emerging technologies and the unique challenges of the urban setting via a broad church of perspectives. Collaboration between professionals of different backgrounds, such as lawyers and information technology (IT) experts, is essential to anticipate challenges and ensure that new technology complies with IHL. Diverse technical expertise may also be required in the field, such as consultation with cities experts and engineers to determine the anticipated harm caused by attacks in complex urban environments.

Cyber warfare

All States are reliant on cyber-space to a greater or lesser extent; civilian, private industry and military activities are increasingly performed online. In urban areas in particular, the interconnectedness of these networks, and of supporting kinetic infrastructure, creates challenges for the fundamental principle of distinction and in the assessment of proportionality. In a recent US Cyber Command report, referenced in the session, the United States predicts that the future of warfare is in cyberspace.³

Increasing capacity (on the part of both State and non-State actors) to pursue military aims using cyber means raises concerns about indiscriminate use, particularly in the hands of parties who consistently display a willingness to violate IHL. Conversely, the digital domain presents an opportunity to record and publish violations in real time through platforms such as social media.

The definitional challenges identified by participants as relevant to the cyber sphere were confined to the need to disseminate an existing vocabulary between disciplines and to promote public understanding. As an example, it was noted that the term “cyber-warfare” in the legal sense denotes a context in which *jus in bello* applies, but is widely used in other fields and in the media to refer to a much broader range of cyber activities.

Military uses of cyber-technology bear inherent relevance to urban settings given their concentration of networked infrastructure. Weaponization of and targeting in the cyber domain could pose particular concerns in urban theatres, where the effects of conflict on the civilian population are already severe. The resilience of such populations to new forms of attack is already degraded by the

2 See, further, Michael Schmitt, “Precision Attack and International Humanitarian Law”, *International Review of the Red Cross*, Vol. 87, No. 859, 2005.

3 US Cyber Command, “Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command”, March 2018, available at: <https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf> (all internet references were accessed in July 2018).

protracted nature of modern conflict. Cyber presents an ability to target infrastructure in new ways and could intensify vulnerabilities to the incidental effects of attack, whether to the civilian use of potentially dual-use objects such as the electricity grid or transportation networks or to civilian and specially protected objects such as banking institutions and health facilities.

Legal issues

IHL applies to cyber-warfare, including the rules governing the conduct of hostilities, but many challenges in interpretation and application of the law remain.⁴ Calls have been made for a new treaty to regulate cyber-space; for example, Microsoft president Brad Smith is an advocate for a “digital Geneva Convention”.⁵ Participants were sceptical about the prospects of such a binding instrument, expressing doubts as to its ability to gain State consensus and endorsement, and concerns about the effect of a potentially low opt-in rate. Further, the prevailing view was that current law is actually sufficient to deal with issues in cyber-space, and that the true challenge lies in the application of and compliance with this law. The roundtable identified the value of international guidance and fora such as the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Tallinn Manual) and the United Nations Group of Governmental Experts on Developments in the Field of Information Security and Telecommunications in the Context of International Security (UN GGE on Information Security). This is not to deny that there might be a need to develop the law further as technologies evolve or their humanitarian impact becomes better understood.

Applicable law

On the threshold issue of the applicability of international law to cyber operations, it was noted that the academic discussion may have progressed further than State practice. The position of the Australian government, set forth in the Australian International Cyber Engagement Strategy,⁶ is that international law applies without reservation to cyber operations. This view is compatible with that of the Tallinn Manual’s group of international experts but is in contrast to some of the views expressed during the 2016/17 meetings of the UN GGE on Information Security. The UN GGE on Information Security failed to reach a consensus on the applicability of key areas of international law to cyber-space.

4 See ICRC, “International Humanitarian Law and the Challenges of Contemporary Armed Conflicts”, *International Review of the Red Cross*, Vol. 97, No. 900, 2015, pp. 1473–1475.

5 See Brad Smith, “The Need for a Digital Geneva Convention”, *Microsoft On the Issues*, 14 February 2017, available at: <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/>.

6 Commonwealth of Australia, Department of Foreign Affairs and Trade, “Australia’s International Cyber Engagement Strategy”, October 2017, available at: http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/pdf/DFAT%20AICES_AccPDF.pdf.

This lack of agreement amongst States, on such fundamental principles, creates a level of ambiguity which can be exploited by international actors deliberately operating in a space without clear, accepted parameters. There is a so-called “grey zone” in which actors are able to conduct cyber operations that fall short of a use of force but that nonetheless generate significant harmful effects. This has implications for the use of lawful countermeasures (for example, whether force can legitimately be used in self-defence) in response and creates legal uncertainty for States responding to cyber threats. One participant raised the possibility of applying a “doctrine of accumulation” in relation to cyber activities, whereby multiple acts over a period of time, which individually fail to constitute a use of force, may, taken in combination, reach the requisite threshold. In this participant’s view, such an approach could be extrapolated as an extension of International Court of Justice (ICJ) cases such as *Nicaragua*⁷ and *Armed Activities*.⁸

Proportionality and precautions

The complex environment of cities presents difficulties in accounting for the reverberating effects of cyber-attacks and raises questions about the extent of obligations to avoid or at least minimize incidental harm. One participant drew an analogy with the use of explosive weapons in densely populated urban areas and proposed that there is an obligation on parties to refrain from launching cyber-attacks in such environments, where their effects cannot be contained or predicted. In any case, there was general consensus that not only primary effects but also foreseeable reverberating effects must be included in the assessment of expected loss of civilian life, injury to civilians and damage to civilian objects required by the principle of proportionality. Experts agreed that an assessment of only the primary effects of weapons is particularly inadequate in the urban setting, and would be contrary to the letter of IHL.

Questions were posed probing the limits of the proportionality assessment of cyber-attacks conducted against targets located in urban areas: if cyber-security measures may make it more difficult for commanders to anticipate or understand the direct and indirect effects of an attack, how do these security measures affect the obligation to assess “expected” incidental loss? How does a nation equip and train a commander to understand this? As cyber-attacks can be re-engineered by other parties, should this be taken into account when an attack is launched and, if so, how?

Responses to such questions focused on the need for commanders to consult, prior to launching a cyber-attack and to the extent feasible, with experts not only in IT but across disciplines including urban planning and water engineering. The feasibility of consultations would be greater in a deliberate targeting situation than in a dynamic one.

7 ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Judgment, 26 November 1984.

8 ICJ, *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Judgment, 19 December 2005.

Attribution

The nature of the cyber domain creates practical and legal difficulties for attribution. Despite this challenge, participants noted the United Kingdom and United States' recent public attribution of the "NotPetya" cyber operation to Russia (which Russia denies).⁹ Some suggested there may be a deterrent value in such attribution. At the same time, some experts voiced concerns that attribution in the absence of visible punitive measures is of limited value (and, indeed, could be perceived as acquiescence, which risks setting a dangerous precedent). However, they cautioned that States should not be hasty in attributing actions in the face of significant ambiguity. It was noted that some members of the UN GGE on Information Security had raised the possibility of funding a body with the role of investigating cyber incidents and producing a report, in part to overcome issues of attribution. Participants suggested a number of reasons why the proposal had failed to receive support: the lack of positive precedent;¹⁰ the cost of establishing and running such a body; the unwillingness of States to relinquish their best cyber experts to the organization; and the objection to investing in an organization which could be seen as reactive rather than preventative.

Positive uses in armed conflict

Cyber means could mitigate the effects of an attack by minimizing kinetic force (for example, reducing the blast and fragmentation effects of explosive weapons, and the resultant debris) and thus the associated incidental loss of civilians and civilian objects. This is especially pertinent to cities, where military and civilian objects and personnel are closely intermingled and the effects of kinetic weapons may be difficult or even impossible to contain.

Cyber-capabilities may also increase the feasible precautions available to a party conducting an attack – for example, by expanding the ability to map an area and allowing the party to input a greater range of data into its Collateral Damage Estimates. In complex urban environments, this may enable a belligerent to better account for civilian movement and to more widely and effectively distribute warnings about military operations to personal devices.

One participant took the view that cyber-capabilities may also increase the opportunities for a defender to minimize harm to civilians, such as by live-publishing data to the adversary on the location of humanitarian evacuation corridors or providing access to CCTV feeds in areas with dense civilian activity. This would increase the information available to a commander to inform precautionary measures and avoid civilian casualties, as well as removing a level of deniability in the event of violations.

9 See Sarah Marsh, "US Joins UK in Blaming Russia for NotPetya Cyber-Attack", *The Guardian*, 15 February 2018, available at: www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine.

10 See, for example, the tendency of some States to discredit reports by the Organisation for the Prohibition of Chemical Weapons, which could be considered as a model for such an investigative body.

New robotics

Participants spoke of the inevitable increased integration into the military of robotics and artificial intelligence in the coming decades. The session on new robotics centred on the development of autonomous systems and particularly on the issues raised by autonomous weapon systems. These weapon systems raise questions about when, and to what degree, human involvement is ethically and legally necessary in the use of force.

On the one hand, the ability of robotics to rapidly process large quantities of data and to provide precision targeting may be beneficial in reducing incidental loss to non-military personnel and objects. On the other, distance from a victim (including physical, psychological and mechanical distance) has been shown to lower inhibitions to the use of lethal force,¹¹ which may have ramifications for the number of casualties (military and civilian). A related concern is whether, by reducing the human cost to a party in the form of troop casualties, the use of such systems could actually reduce incentives for resolution and result in a more protracted conflict. Fears were also raised about the possibility of rogue or hacked robots performing indiscriminate attacks.

Finally, it was noted that the operators and programmers of autonomous weapon systems will not necessarily be military personnel, complicating the distinction between combatants, civilians and civilians directly participating in hostilities.

Legal issues

Definitional issues were discussed, including the ICRC's proposed umbrella term of "autonomous weapon systems".¹² One contributor expressed discomfort with the idea of defining autonomous weapon systems prior to clarifying the issue which needs to be regulated and working backwards from this point. For example, is the main concern protecting the dignity of combatants, preservation of civilian life, or preventing the accumulation of an asymmetric advantage in conducting warfare? The answer may affect the specific definition that is adopted for that regulatory purpose.

Proponents at the roundtable suggested that robotic systems could be programmed to reduce casualties and eliminate biases. However, others were concerned that, even with machine learning, these systems will never have the

11 See, for example, David Grossman, *On Killing: The Psychological Cost of Learning to Kill in War and Society*, Back Bay Books, New York, 1995, Section III and Section IV Ch. 3.

12 The ICRC has proposed that "autonomous weapon system" is an umbrella definition for any weapon system with autonomy in the critical functions of selecting and attacking targets. See ICRC, *Convention on Certain Conventional Weapons (CCW) Meeting of Experts on Lethal Autonomous Weapons Systems, 11–15 April 2016: Views of the International Committee of the Red Cross (ICRC) on Autonomous Weapon System[s]*, Geneva, 11 April 2016, available at: www.icrc.org/en/document/views-icrc-autonomous-weapon-system. See also ICRC, "Autonomous Weapon Systems under International Humanitarian Law", 31 January 2018, available at: www.icrc.org/en/document/autonomous-weapon-systems-under-international-humanitarian-law.

capacity to apply rules such as distinction and proportionality, which require an element of subjective judgement that cannot or should not be satisfied by an algorithm. Indeed, it is the ICRC's position that only humans can apply IHL.¹³ Without the ability to be used in compliance with these rules, such robots would be prohibited by existing IHL, thus perhaps negating the need to develop an autonomous weapon system-specific prohibition.

Accountability

Initially, several participants queried the ability to apply legal accountability mechanisms such as individual and command responsibility to a violation resulting from the use of an autonomous weapon system. By the end of the session there was general agreement that autonomy in robotic systems was not likely to actually pose an obstacle to international criminal law. It was felt that the use of force could always be traced back to a human commander or operator making the decision to deploy the weapon, or at the most distant degree of control, to a human programmer.

A moral obligation to use new technologies?

The hypothetical was given of a comparable rate of 80% human accuracy with a non-autonomous weapon system in striking the correct target and a 20% rate of error putting civilians and civilian objects at risk, versus a machine with respective 95% and 5% accuracy rates. Where use of the machine results in greater compliance with IHL than the human with a non-autonomous weapon but nonetheless also results in errors, some questioned whether the quest for the perfect system was overshadowing the possible benefits in reduced civilian casualties and infrastructure damage.

A handful of participants went so far as to query whether there is a legal obligation, based on the requirement to take precautions and the restriction on choice of means and methods of warfare, to employ autonomous weapon systems where their use can deliver superior reliability to humans using non-autonomous weapon systems.

Positive uses

Optimism was expressed for the potential benefits of autonomous systems in urban areas, where robots may be able to process and analyze data faster than their human counterparts. This is salient considering the complexity of the built environment, where the co-mingling of civilians and combatants presents difficulties for applying distinction and conducting evacuations, and creates many options for defenders to conceal themselves. Urban fighting has a tendency to break forces into small units and can produce particularly brutal close-combat fighting. The ability to design artificial systems not to engage in self-defence and to fire only

13 See ICRC, "Towards Limits on Autonomy in Weapon Systems", Statement, 9 April 2018, available at: www.icrc.org/en/document/towards-limits-autonomous-weapons.

after being fired upon were identified as potential assets in these settings. Fixed or area-restricted autonomous systems could avoid driving combat into homes, and robots would not necessarily require the same air support as human troops, thus reducing one of the largest contributors to incidental loss to civilian life and infrastructure in urban conflict.

Human enhancement

The enhancement of human capability is not a new phenomenon in armed conflict. The roundtable cited the use of the methamphetamine Pervitin by the German armed forces in the Second World War as one historical example, but emphasized that scientific advances have greatly increased the range of possible enhancements.

Participants noted that determining what falls within the definition of an enhancement can be difficult, given that a state of normality is highly variable and subjective, and that the effects and intended use of the technologies are very diverse. Furthermore, some enhancement techniques can also be used as therapy in the process of restoring a human to normal ability, such as techniques to improve soldiers' resilience to disease, injury or psychologically traumatic events.

It was queried whether the term "human modification" should be preferred over "human enhancement", to avoid the assumption of an inherently beneficial process. One speaker suggested that human modifications can generally be separated into three categories: physical modifications which alter characteristics such as endurance or the senses; psychological modifications which impact a person's emotional processes, for example relating to aggression or trauma; and cognitive modifications which affect intelligence and decision-making ability, attention, memory, and acquisition of new skills.

Whilst no definition was nominated, it was generally agreed that behaviour modification techniques such as training exercises and military conditioning do not fall within the scope of enhancements and that biomedical intervention would be required to justify inclusion in that category.

Although the forum was an opportunity to explore the connections between emerging military technologies and urban settings, experts found that the characteristics of the urban environment did not bear specific relevance to the issues raised by human enhancement.

Ethical issues

A variety of ethical issues were flagged, arising at distinct stages: the process of undergoing modification, during deployment, and following return to civilian life. Given that obedience to the military hierarchy may undermine the voluntariness of consent, one expert proposed that a higher threshold than informed consent should be required for members of the armed forces to undergo enhancement procedures. Some felt that modifications should only be permitted when

reversible and were also concerned about the ability of modified fighters to reintegrate, including due to the effects of the removal of the modification.

Legal issues

IHL and international human rights law

Experts accepted that IHL is generally not concerned with regulating the treatment of a party's own forces.¹⁴ Therefore a domestic law approach, informed by the human rights framework, would be most applicable to the protection of combatants from coercion and risk associated with human modification. The processes of modification and reintegration also mostly occur outside of the context of an armed conflict, where IHL will not apply.

Ability to comply with IHL

Concerns were raised about the impact of cognitive and psychological modifications upon a person's ability to make subjective judgements and therefore to apply IHL rules, notably those of proportionality and distinction. Again, the issue of distance was discussed, with concerns raised that altering emotions may produce a level of psychological distance which could reduce resistance to killing.

Article 36 review

It was generally accepted that it would be problematic, both from a legal and a humanitarian point of view, to classify an enhanced human as a "weapon" rather than as a "combatant". Nevertheless, it was considered possible that some modifications may fall within the review requirements of Article 36 of AP I, either as a means or a method of warfare. For example, if an implanted device were a component of a weapon system, such as a brain-computer interface, it might constitute a "means" of warfare, while a psychoactive drug that increases aggression could be a tactical "method".

One speaker made the argument that, irrespective of any possible legal duty to review human enhancements, there is a good policy argument to do so given the sensitive ethical issues around human modification that will likely place a strain on civil-military relations. A transparent and thorough review process could assist with building assurance within government and with the public.

In response to the concern that it could be practically difficult to review an embedded modification due to the variability of the controlling human, it was noted

14 Noting that there are exceptions for certain acts such as rape and sexual slavery: see International Criminal Court, *The Prosecutor v. Bosco Ntaganda*, Case No. ICC-01/04-02/06-1962, 15 June 2017. See also *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 2nd ed., Geneva, 2016, Art. 3, paras 547–549.

that conventional weapons may also be used differently according to the user, and that training can function as a form of standardization.

Medical personnel

Though the majority of the discussion focused on the modified soldier, one speaker called attention to the possible consequences for medical personnel called upon to administer or supervise the use of modifications. The question was posed (without answer) that if medical personnel closely supervise the application of enhancements, could they be said to be performing acts harmful to the adversary and thus be stripped of their protection from targeting under IHL?

Countering enhanced personnel

Another issue identified relates to weapons deployed to counter modified humans. Firstly, should enhancements be taken into account for the purposes of assessing superfluous injury and unnecessary suffering? For example, would it be permissible under IHL to deploy a weapon against a soldier who has been modified to have a higher pain tolerance when that weapon would otherwise fall foul of the prohibition on weapons of a nature to cause superfluous injury or unnecessary suffering? Secondly, as weapons are generally regulated under IHL by virtue of their primary effects, how might counter-modification weapons affect “normal” humans who are not the primary target?

One speaker noted that the only explicit reference to human enhancement in IHL is found in Protocol IV to the 1980 Convention on Certain Conventional Weapons (also known as the Protocol on Blinding Laser Weapons), which prohibits weapons with the combat function of causing blindness to *unenanced* vision, “that is to the naked eye or to the eye with corrective eyesight devices”.¹⁵ It was posited that a risk existed that weapons whose combat function was to counter enhanced vision would not be prohibited by the protocol.

Positive uses

Some participants viewed human modification techniques as potentially creating more humane conditions for combatants. Examples included modifying memory associations to reduce trauma, as well as increasing the survivability of fighters. One contributor wondered whether an argument could be made in favour of an *obligation* to modify soldiers, drawing an analogy with the ruling of the UK courts that the UK government was obliged to properly equip soldiers as an aspect of the right to life under the European Convention on Human Rights.¹⁶

15 CCW, Protocol IV (Protocol on Blinding Laser Weapons), 13 October 1995, Art. 1.

16 UK Supreme Court, *R (on the Application of Smith) (FC) (Respondent) v. Secretary of State for Defence (Appellant) and Another*, [2010] UKSC 29, 30 June 2010.

New technology and military and policy decision-making

Decisions to regulate new technologies

There was universal agreement that the existing IHL framework regulates these new technologies in armed conflict. However, as technologies develop, further clarification and development of the law may be needed to address certain challenges. In the context of developing regulatory frameworks for new technologies, one speaker highlighted the need to first clarify what is sought to be achieved and the basis of any intuitive objections to the use of new technologies. This requires us to interrogate issues such as: is the regulation directed at the technology itself, or at its effects, or even at a broader aim such as increased participation in decision-making or non-proliferation? Who are we seeking to regulate? And is a legal solution the most appropriate for the issue, or could it have unintended or inappropriate consequences (for example, in the case of a complete ban)?

Military decision-making

One speaker outlined key aspects of the military decision-making process that are relevant to the broader discussion of new technologies in armed conflict. At the development and acquisition phase, these include evaluations of civilian expectations of the military and weapons reviews conducted pursuant to Article 36 of AP I. Force composition decisions then guide deployment of any weapon systems, and strict rules ultimately continue to regulate the use of force by any technology. It was argued that, too often, this context is left out of discussions such as those in the UN GGE in relation to autonomous weapon systems.

Applying these considerations to autonomous weapon systems, it was noted by one participant that, to be militarily effective, these systems must be able to operate in a bounded way to deliver controlled violence. This is necessary not only for reasons of predictability and planning, but also to ensure that the military's use of force retains a level of moral and social legitimacy.

Referring to this element of predictability required for military efficacy, one participant queried how this might be affected by “black box” decision-making. That is to say, if the decision-making process of a weapon system was completely opaque such that it made the correct decision 99% of the time but it was not possible to ascertain why it did so, could this weapon system be assessed as sufficiently predictable? Such considerations also pose interesting questions in the context of Article 36 reviews.

Another expert took up the idea of accountability systems and mechanisms, and their potential to play a role in alleviating social concerns and calculating public morays. Established firm parameters were flagged as particularly important given that new technology will likely be widely and cheaply available in the future and not restricted to conventional militaries.

Conclusions

As one participant noted, “as a lawyer I always think the law is sacrosanct and all I have to do is hand someone the law”. However, there is a need to look beyond the law to the ethical and policy considerations which should also inform decision-making. The roundtable prompted questions as to what role humans should play amidst increasing automation. Compassion, a sense of fairness and justice, a moral check and balance: these may not be qualities which we can mechanize. At the same time, some discussions challenged the concept of the human as the ideal; perhaps there are tasks and decisions which may be better performed and made by machines. On the other hand, there may also be decisions – especially judgments regarding compliance with international humanitarian law – that must be taken by humans. Similarly, increasingly autonomous systems and modified soldiers present regulatory and ethical challenges but offer opportunities in both military and humanitarian applications.

Hopes were expressed that legal developments and accountability mechanisms around emerging technology will be both proactive and grounded in strategic and operational realities. Especially in light of the need to anticipate future uses (and possible abuses), experts praised a multidisciplinary approach, which combines technical knowledge with humanitarian, military, governmental, academic and civil perspectives.

There is still some way to go to reach comprehensive and widely accepted definitions in complex areas such as human modification. Some of the difficulty in distilling the most appropriate definitions was identified as stemming from uncertain or competing directions of potential regulation. As discussions progress and the technologies continue to develop, regulatory priorities will become clearer.

There is need for greater compliance with extant law, and significant value in fora and expert guidance such as the UN GGEs and the Tallinn Manual. IHL is equipped to set parameters around the use of new technologies, and its principles and rules continue to be fundamentally relevant, although further clarification and development of the law may be needed to address certain challenges raised by these technologies.

The potential of new technologies to reduce casualties and assist humanitarian operations, such as evacuations and medical relief activities, provide a positive counterpoint to the concerns raised. In the increasingly urban setting of modern conflicts, it is hoped that such capabilities will contribute to preservation of civilian life and infrastructure where dense populations are at greatest risk from the reverberating effects of attacks.