Melbourne Law School

Melbourne Legal Studies Research Paper
No. 721

Emerging Technologies of Warfare

Rain Liivoja, Kobi-Renée Leins and Tim McCormack

This paper is forthcoming in the
Routledge Handbook of the Law of Armed Conflict, R Liivoja and T McCormack (eds)
Routledge

35
Emerging Technologies of Warfare

RAIN LIIVOJA, KOBI-RENÉE LEINS and TIM McCORMACK*

Advances in science and technology have had a major impact on the conduct of war throughout history.[1] On a popular view, the development of warfare has been punctuated by so-called 'revolutions in military affairs', periods of rapid change in military thinking and practice; scientific and technological transformations have played a significant role in such change.[2] At the time of writing, we appear to be in the midst of one revolution in military affairs, namely an information revolution.[3] This revolution has been facilitated by the development of digital computers and their wide adoption in the society at large and in military systems in particular.

Assuming that there is an ongoing revolution in military affairs, the question arises as whether it ought to be accompanied by a 'revolution in military legal affairs',[4] or whether the existing law of armed conflict (LOAC) is capable of accommodating recent technological developments. This chapter does not purport to provide a comprehensive answer to this question nor does it seek to evaluate the lawfulness or otherwise of specific means or methods of warfare. Rather, it addresses some of the key legal implications and regulatory challenges arising from the military applications of a certain types of technology.[5] We begin with information technology and the notion of 'cyber warfare' (Section 1). We then turn to robotics, specifically remotely controlled, automated and autonomous military systems (Section 2). Finally we consider nanotechnology (Section 3). We concluded the chapter

* The research for this chapter was supported under Australian Research Council's *Discovery Projects* funding scheme (project number DP130100432) and by a Society in Science – Branco Weiss Fellowship (administered by ETH Zurich). We are grateful to Chris Jenks, Natalia Jevglevskaja, Robert J Mathews, Tim McFarland and Angus Willoughby for comments on an earlier draft. The responsibility for the present text, however, remains ours.

[1] See generally Martin van Creveld, *Technology and War: From 2000 BC to the Present* (rev edn, Free Press 1991); Max Boot, *War Made New: Technology, Warfare, and the Course of History, 1500 to Today* (Gotham Books 2006).

[2] See the seminal work by Michael G Vickers and Robert C Martinage, 'The Revolution in War' (Center for Strategic and Budgetary Assessments, December 2004).

[3] Boot (n 1) 305 et seq.

[4] This term has been used, although not specifically in relation to technology, by Charles J Dunlap Jr, 'The Revolution in Military Legal Affairs: Air Force Legal Professionals in 21st Century Conflicts' (2001) 51 *Air Force Law Review* 293.

[5] For other broad discussions, see, eg, Special Issue: New Technologies and Warfare (2012) 94(886) *IRRC* 457; Dan Saxon (ed), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff 2013); Hitoshi Nasu and Robert McLaughlin (eds), *New Technologies and the Law of Armed Conflict* (Asser 2014).

Rain Liivoja and Tim McCormack (eds),
Routledge Handbook of the Law of Armed Conflict (Routledge, forthcoming)

Electronic copy available at: http://ssrn.com/abstract=2679669

with a brief reflection on the formal legal review of new means and methods of warfare in the context of emerging technologies of warfare (Section 4).

1 Information technology

1.1 Technology

The start of the ongoing information revolution in military affairs can be reasonably precisely dated to the late 1930s and early 1940s. This was the time when the first digital computers were built, many of which were preoccupied by military tasks such as ballistics calculations and code breaking.[6] Of course, computers have developed quite spectacularly from what in hindsight appears to be a rather humble beginning as advanced calculators, into systems that process and store exponentially increasing amounts of data, which is often strategically significant and/or economically valuable.

Also, computers are widely used to exert control over the physical world. Computerised industrial control systems (ICS) are common in many different sectors of industry and infrastructure.[7] A comparatively simple programmable logic controller (PLC) can run a specific device – such as an elevator, a set of traffic lights, or an industrial appliance – by 'monitor[ing] the state of input devices and make[ing] decisions based upon a custom program to control the state of output devices'.[8] A distributed control system (DCS) is more complex, coordinating between multiple sub-systems involved in carrying out an entire industrial process, for example at an oil refinery, water and wastewater treatment plant, power plant or chemical manufacturing plant.[9] Another type of ICS, a supervisory control and data acquisition (SCADA) system, is 'designed to collect field information, transfer it to a central computer facility, and display the information to the operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a central location in near real time'.[10] SCADA systems are widely used in distribution systems, such as water distribution and wastewater collection systems, oil and natural gas pipelines, electrical grids, as well as rail, air traffic control and other public transportation systems.[11]

Computers are routinely connected to each other to form networks. These networks can, in turn, be connected to other networks, ultimately making up the Internet. This allows for the remote access and manipulation of data, such as accessing a website stored on a server or

---

[6] See Martin Campbell-Kelly, Willian Aspray, Nathan Ensmenger and Jeffrey R Yost, *Computer: A History of the Information Machine* (3rd edn, Westview, 2013).

[7] Keith Stouffer et al, 'NIST Special Publication 800-82 – Guide to Industrial Control Systems (ICS) Security', Revision 2 – Final Public Draft (National Institute of Standards and Technology, US Department of Commerce, February 2015).

[8] Advance Micro Controllers Inc, 'What Is A Programmable Logic Controller (PLC)?' (undated) http://www.amci.com/tutorials/tutorials-what-is-programmable-logic-controller.asp.

[9] Stouffer et al (n 7) 2-10.

[10] ibid 2-5.

[11] ibid.

Electronic copy available at: http://ssrn.com/abstract=2679669

saving documents in the 'cloud'. ICS are also often networked. Indeed, the architecture of DCS and SCADA presumes a degree of interconnection between computers. Also, many ICS are connected to the Internet to facilitate remote access. The same is true for various computerised devices, ranging from mobile phones to refrigerators – giving rise to the phenomenon referred to as the 'Internet of Things'.[12]

Computers and networks have vulnerabilities, that is to say flaws or weaknesses in their design or operation, which can be exploited to violate information systems' key security attributes – confidentiality, integrity or availability.[13] A breach of confidentiality entails access to data by an unauthorised person, for instance for the purposes of cyber espionage. This was the case with the alleged copying by Chinese hackers of sensitive design data of the US's F-35 Joint Strike Fighter[14] and the blueprints of the new headquarters of the Australian Secret Intelligence Organisation.[15] A breach of integrity involves the modification of data on the system or the system's configuration. This would include the defacement of websites, as well as the loading by hackers of pro-ISIS videos and messages to the US military's YouTube and Twitter accounts.[16] A violation of availability denies access to data, of services of the system, to those authorised to use them. An example would be the launch of such a number of queries to a system as to overwhelm it and to shut it down or to render it inaccessible, referred to as a denial-of-service attack. Prominent examples include the disabling of governmental websites of Estonia (in April 2007), Georgia (in July–August 2008) and Germany (in January 2015) by cyber activities ostensibly emanating from Russia.[17]

Perhaps more seriously, given the wide use of computerised ICS, cyber operations altering data can provoke real-world physical events. The most prominent example was the use of the Stuxnet virus to infect the ICS of an Iranian uranium enrichment facility; the virus manipulated the rotational speeds of centrifuges, causing them significant damage.[18] It does

---

[12] See, eg, Dave Evans, 'The Internet of Things: How the Next Evolution of the Internet is Changing Everything', White Paper (Cisco Internet Business Solutions Group, April 2011); Jacob Morgan, 'A Simple Explanation of "The Internet Of Things"', Forbes (13 May 2014) <http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand>.

[13] See, eg, George Loukas, *Cyber-Physical Attacks: A Growing Invisible Threat* (Butterworth-Heinemann 2015) 2–3.

[14] See Siobhan Gorman, August Cole and Yochi Dreazen, 'Computer Spies Breach Fighter-Jet Project', *The Wall Street Journal* (21 April 2009).

[15] See Ben Grubb, 'Blueprints for new ASIO headquarters "stolen"', *The Age* (Melbourne, 27 May 2013).

[16] See Mana Raibee, 'US Central Command's YouTube, Twitter Accounts Suspended after Hacking by IS Supporters', *The New York Times* (12 January 2015) <http://www.nytimes.com/video/multimedia/100000003445205>.

[17] See Michelle Martin and Erik Kirschbaum, 'Pro-Russian Group Claims Cyber Attack on German Government Websites', *Reuters* (7 January 2015) <http://www.reuters.com/article/2015/01/07/us-germany-cyberattack-idUSKBN0KG15320150107>.

[18] See, eg, Holger Stark, 'Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War', *Der Spiegel International* (8 August 2011)

not require much imagination to envision the potentially catastrophic destruction that could be caused by cyber operations against air traffic control systems, emergency services, dams or nuclear power plants.

1.2 Legal challenges

Since the late 1990s, significant effort has gone into clarifying the international legal framework applicable to hostile cyber operations. Numerous papers and books have appeared on the law of cyber warfare,[19] with the most prominent scholarly publication being the 2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare*,[20] a statement of 95 rules considered to be *lex lata* by an international group of experts meeting at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence.[21]

There appears to be broad agreement on a few important issues. Most fundamentally, hostile cyber operations undertaken by belligerents in the context of an ongoing armed conflict are, like other military operations, governed by LOAC.[22] In particular, where such cyber operations amount to 'attacks' within the meaning of LOAC, they are subject to the key principles of distinction and proportionality, and necessitate the taking of certain precautionary measures.[23]

These general propositions, however well accepted, inexorably lead to further questions. First, which cyber operations amount to 'attacks'? Second, are cyber operations that do not amount to attacks subject to restrictions of LOAC? Third, are cyber operations capable of

---

<http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html>.

[19] See, eg, symposia in (2012) 17 *JCSL* 183, (2013) 84 *International Law Studies* 1; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (CUP 2012); Marco Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014); Jens David Ohlin, Claire Finkelstein and Kevin Govern (eds), *Cyber War: Law and Ethics for Virtual Conflicts* (OUP 2015).

[20] *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013) <https://ccdcoe.org/tallinn-manual.html>.

[21] For critical comments, see, eg, Rain Liivoja and Tim McCormack, 'Law in the Virtual Battlespace: The Tallinn Manual and the *Jus in Bello*' (2012) 15 *YBIHL* 45; Dieter Fleck, 'Searching for International Rules Applicable to Cyber Warfare: A Critical First Assessment of the New Tallinn Manual' (2013) 18 *JCSL* 331; Oliver Kessler and Wouter Werner, 'Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare' (2013) 26 *Leiden JIL* 793.

[22] See ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflict', 31st International Conference of the Red Cross and Red Crescent, 28 November–1 December 2011, Doc 31IC/11/5.1.2 (October 2011) 38; *Tallinn Manual* (n 20) r 20; for further references, see David Turns, 'Cyber War and the Concept of "Attack" in International Humanitarian Law' in Saxon (ed) (n 5) 209, 221 (citing academic works), Cordula Droege, 'Get Off my Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94(886) *IRRC* 533, 567 (citing views of states), and Roscini (n 19) 21–22 (citing views of states).

[23] See ICRC (n 22) 37; *Tallinn Manual* (n 20) rr 31, 51, 53–59.

triggering the application of LOAC in the absence of 'ordinary' hostilities? While we readily acknowledge that a number of further LOAC issues arise from cyber operations, we limit our attention here to these three key questions as they are in some ways foundational to any discussion about the law of cyber hostilities.

1.2.1 Cyber operations as 'attacks'

Additional Protocol I defines 'attacks' as 'acts of violence against the adversary, whether in offence or defence'.[24] According to the prevailing view, it is the anticipated violent effect or consequence of an act that allow it to be characterised as an attack.[25] Commentators point out that the wilful release of pathogens or toxic chemicals, entailing no overtly violent action, undoubtedly constitute attacks for the purpose of LOAC because of their harmful or even lethal consequences.[26] Thus, the lack of violent action cannot exclude cyber operations from constituting attacks as long as the consequences are violent.

There is broad support for the proposition that injury or death to persons, or damage or destruction to objects, amounts to violence, and that cyber operations that are reasonably expected to have such consequences amount to attacks.[27] On one view, physical damage of this nature is not merely a sufficient but a necessary condition for a cyber operation to constitute an attack.[28] This reading relies on the literal meaning of the word 'violence' and draws support from the formulation of the principle of proportionality in Additional Protocol I, which speaks of 'loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof'.[29] According to an alternative view, the disabling of an object, even without causing any physical damage or destruction, also constitutes an attack.[30] The

[24] API art 49(1).

[25] Michael N Schmitt, 'Cyber Operations and the *Jus in Bello*: Key Issues' in Raul A Pedrozo and Daria P Wollschlaeger (eds), *International Law and the Changing Character of War* (US Naval War College 2011) 89, 93–94; Roscini (n 19) 179; for a detailed discussion, see Turns (n 22) 221–224.

[26] See, eg, Schmitt, 'Key Issues' (n 25) 94; Bill Boothby, 'Where do Cyber Hostilities Fit in the International Law Maze?' in Nasu and McLaughlin (eds) (n 5) 59, 60.

[27] See *Tallinn Manual* (n 20) r 30.

[28] Schmitt, 'Key Issues' (n 25) 94–95; Yoram Dinstein, 'The Principle of Distinction and Cyber War in International Armed Conflicts' (2012) 17 *JCSL* 261, 264.

[29] Michael N Schmitt, 'Wired Warfare: Computer Network Attack and *Jus in Bello*' (2002) 84(846) *IRRC* 365, 376-377.

[30] Knut Dörmann, 'The Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Approach' in Karin Byström (ed), *International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, 17–19 November 2004, Stockholm, Sweden: Proceedings of the Conference* (Swedish National Defence College 2005) 139, 142-143; ICRC (n 22) 37.

proponents of this approach rely in particular on the definition of military objects in Additional Protocol I, which implies that the capture or neutralisation of an object is a possible aim of an attack.[31]

One construction attempts to reconcile these two approaches. This moves the focus from physical destruction to 'the fact that it [the object] is no longer completely suitable for its intended purpose'.[32] It does so by interpreting the notion of 'damage' to mean 'the loss of functionality that permanently renders the object inoperable or that necessitates some form of repair'.[33] However, even amongst those who adopt this approach to 'damage', there is no unanimity as to the nature or extent of the repair necessary. Circumstances where 'restoration of functionality requires replacement of physical components' seems to be more readily accepted as damage.[34] Going further, some would argue, for example, is that the reloading of 'the operating system or any software essential to operation' would qualify as damage; however, replacing data 'merely stored on the system' would not.[35]

This discussion is closely associated with the problem as to whether data could qualify as an 'object'. If that were the case, the destruction of data in itself – that is to say, even in the absence of physical damage or loss of functionality of a device – could be considered an attack. There does not appear to be much support for the data-as-object position.[36] This is unsurprising given that the ICRC *Commentary* to the 1977 Additional Protocols indicates that the word 'object', as used in Additional Protocol I, means 'something that is visible and tangible'.[37] But, as we have argued elsewhere, this corporeal conception of objects under LOAC may be outdated.[38] The economic value of data can be enormous and its permanent destruction may have far more serious consequences than the destruction of some tangible objects. As a result, it may prove difficult in the long run to 'maintain a normative distinction between harm caused to physical objects and that caused to data'.[39]

1.2.2 Cyber operations not amounting to 'attacks'

The vast majority of cyber operations would not meet the fairly restrictive definition of attacks outlined previously. This raises the question whether such operations are subject to any restrictions under LOAC. Notably, Article 48 of Additional Protocol I requires parties

---

[31] API art 52(2).

[32] Michael N Schmitt, 'Rewired Warfare: Rethinking the Law of Cyber Attack' (forthcoming) *IRRC*, FirstView advance access, 15.

[33] ibid.

[34] *Tallinn Manual* (n 20) commentary to r 30, para 10.

[35] Schmitt, 'Rewired Warfare' (n 33) 15.

[36] *Tallinn Manual* (n 20) commentary to r 30, para 6. But see Nils Melzer, 'Cyberwarfare and International Law', UNIDIR Resources (2011) 31.

[37] *AP Commentary* para 2008.

[38] See Liivoja and McCormack (n 21) 53–54.

[39] Schmitt, 'Rewired Warfare' (n 33) 16.

to a conflict to 'direct their operations only against military objectives' and Article 57(1) stipulates that, '[i]n the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects'. There are, however, differences in opinion as to the significance of the use of the ostensibly broader term 'operations' instead of 'attack' in these provisions.

Some commentators do not hold the choice of terminology to be determinative: they argue that the prohibition contained in Article 48 'is not so much on targeting non-military objectives as it is on *attacking* them, specifically through the use of violence'.[40] This view draws contextual support from the position of Article 48 within the Protocol: the provision introduces a series of more specific articles, all dealing with attacks.[41] Also, according to the ICRC *Commentary* on Article 48, 'the word "operations" should be understood in the context of the whole of the Section [on methods and means of warfare]; it refers to military operations during which violence is used, and not to ideological, political or religious campaigns.'[42] If this line of reasoning is accepted, cyber operations not amounting to attacks are not restricted by the principle of distinction and thus 'are permissible against non-military objectives, such as the population.'[43]

Alternative views note that the drafters' choice to use the term operations instead of attack must have some significance. Those views rely on the ICRC *Commentary* on Article 48 which accepts a dictionary definition whereby '"military operations" refers to all movements and acts related to hostilities that are undertaken by armed forces'.[44] This has led to the argument that the applicability of LOAC restraints on cyber operations depends on whether they constitute part of 'hostilities'.[45] Accordingly, given that 'hostilities' is a broader concept than 'attacks', cyber operations 'directly adversely affecting military operations or military capacity' of the adversary must also be subject to restrictions imposed by LOAC.[46]

In line with this interpretation, cyber operations aiming to disrupt or incapacitate an adversary's computer-controlled radar or weapon systems, logistic supply or communication networks may not directly cause any physical damage, but would certainly qualify as part of the hostilities and, therefore, would have to comply with the rules and principles of IHL governing the conduct of hostilities. The same would apply to cyber operations intruding into the adversary's computer network to delete targeting data, manipulate military orders,

---

[40] Schmitt, 'Wired Warfare' (n 29) 376 (original emphasis); see also Turns (n 22) 217; Roscini (n 19) 178.

[41] Schmitt, 'Wired Warfare' (n 29) 376.

[42] *AP Commentary* para 1875.

[43] Schmitt, 'Wired Warfare' (n 29) 376.

[44] *AP Commentary* para 1875.

[45] Melzer (n 36) 27.

[46] ibid 28.

or change, encrypt, exploit, or render useless any other sensitive data with a direct (adverse) impact on the belligerent party's capacity to conduct hostilities.[47]

A variation of this approach relies on the commentary to Article 57, which explains that the term '"military operations" should be understood to mean any movements, manœuvres and other activities whatsoever carried out by the armed forces with a view to combat.'[48] Consequently, in order to be subject to the principles of distinction, proportionality and precaution, a cyber operation must be combat-related, in other words it 'must be associated with the use of physical force, but it does not have to result in violent consequences itself'.[49]

On either of the broader conceptions of 'operations', however, propaganda, espionage and psychological operations – sometimes compared with sub-attack cyber operations – would not be governed by the principles of distinction, proportionality and precaution because they are neither part of hostilities nor undertaken with a view to combat.[50]

To conclude the discussion about the difference between attacks and operations, it is worthwhile to note certain persons and objects enjoy special protection under LOAC. In particular, medical personnel, units and transports must be 'respected and protected'.[51] This prohibition 'includes, but is not limited to the prohibition of attacks'.[52] Accordingly, irrespective of what the correct interpretation of the notions of attack and operation may be, any cyber operation that impedes, prevents or otherwise adversely affects the carrying out of humanitarian functions of medical services – for example, altering the GPS data of a medical aircraft or the digital personal records of patients – is prohibited.[53]

1.2.3 Cyber operations as a trigger for armed conflict

The preceding discussion presupposed that an armed conflict was already in existence. The question remains, however, whether cyber operations, in the absence of hostilities involving conventional military means, could constitute an armed conflict and thus trigger the application of LOAC.

Even though the Geneva Conventions and the Additional Protocols apply, according to their own terms, in 'armed conflict', these treaties do not establish what constitutes such a conflict.[54] The now-standard threshold test, reflecting the relevant treaty provisions and customary law, was formulated by the ICTY Appeals Chamber in *Tadić* as follows:

---

[47] ibid 28 (footnotes omitted).

[48] *AP Commentary* para 2191.

[49] Harrison Dinniss (n 19) 201.

[50] See Droege (n 22) 556.

[51] See, in particular, API arts 12(1), 15(1), 21, 23(1), 24; cf *Tallinn Manual* (n 20) rr 70–71.

[52] See *Tallinn Manual* (n 20) commentary to r 70, para 4.

[53] See ibid commentary to r 70, para 4; commentary to r 71, para 3.

[54] See GCI–IV common arts 2 and 3; API art 1; APII art 1.

> An armed conflict exists whenever there is a resort to armed force between States or protracted violence between governmental authorities and organized armed groups or between such groups within a State.[55]

The application of this test to establish the existence of an armed conflict involves, however, a significant preliminary question of attribution. The usual rules of state responsibility apply when determining whether a cyber operation is attributable to a state but demonstrating the requisite link between the operation and a state or a non-state armed group can be difficult.[56] It may well be that cyber operations are undertaken by independent 'hacktivists' whose conduct cannot be attributed to any state or a non-state armed group, in which case a situation of armed conflict would not arise, irrespective of the extent of damage caused.

If the attribution problem can be overcome, the question is whether the requirements of the *Tadić* test can be met.

According to the prevailing view, no particular degree of violence or intention is required for the existence of an international armed conflict – all that is necessary is 'a resort to armed force between States'.[57] On this view, where a single cyber operation, launched by one state against another, amounts to an 'attack' as discussed previously, an international armed conflict would be triggered.[58] Admittedly, the uncertainty as to what constitutes an attack in the cyber context would obviously create some difficulties in this context. But were one to accept the competing view that the applicability of LOAC requires a greater extent, duration or intensity of hostilities, even the 2010 Stuxnet operation, which succeeded in causing physical damage centrifuges in a nuclear fuel processing plant, would not be sufficient to trigger an international armed conflict.[59]

The threshold for a non-international armed conflict is higher: the armed force used must have a certain degree of intensity – in the words of the ICTY, 'protracted violence' – and each non-state armed group involved must have a certain level of organisation.[60] To amount to protracted violence, 'cyber attacks have to be frequent enough to be considered related, [but] they clearly do not have to be continuous'.[61] The requirement of organisation means, for example, that a number of individuals sharing a common purpose, but engaging in cyber operations against a state or a non-state armed group independently of each other, would

---

[55] *Prosecutor v Tadić (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction)* (Case no IT-94-1, ICTY Appeals Chamber, 2 October 1995) para 70.

[56] See, eg, Marco Roscini, 'Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations' (2015) 50 *Texas International Law Journal* 233.

[57] See further Caitlin Dwyer and Tim McCormack, 'Conflict Characterisation', ch 3 in this volume, s 2.2.

[58] See, eg, Michael Schmitt, 'Classification of Cyber Conflict' (2012) 17 *JCSL* 245, 251–2; see also Roscini (n 19) 134–135.

[59] See *Tallinn Manual* (n 20) commentary to r 22, paras 12, 14.

[60] See further Dwyer and McCormack (n 57) s 2.3.

[61] Schmitt, 'Classification' (n 58) 258; see also Roscini (n 19) 152–153.

not constitute an organised armed group.[62] However, a group that operates as a unit in a coordinated fashion – for example where members of the group have assigned roles and they act upon orders issued virtually from a recognised leader – could be seen as organised, even though the members never meet face to face and may never even discover each other's true identity.[63] An additional difficulty is created, however, by Additional Protocol II: Article 1(1) of the Protocol presumes that an organised armed group is 'under responsible command'. This requirement has been interpreted to mean that the organised armed group 'must be in a position to implement the Protocol'[64] and that this entails 'the possibility to impose discipline'.[65] There is obvious doubt whether a group organised virtually would have the tools to impose the kind of discipline that is typical of military organisations. However, there is room for the argument that the 'responsible command' requirement does not limit the applicability of Common Article 3,[66] and that, at any rate, 'being in a position to implement' the law merely requires 'the organisational *ability* to comply with the obligations of international humanitarian law'.[67]

Whatever the correct interpretation, the intensity and organisation requirements imposed by the LOAC of NIACs are significant. Thus the plausible view has been expressed that 'cyber operations alone can trigger a non-international armed conflict in only rare cases.'[68]

2 Robotics

2.1 Technology

The term 'robotics' refers to 'the science and technology of robots'.[69] There is a modicum of agreement that a robot is 'an artificial device that can *sense* its environment and *purposefully act* on or in that environment'.[70] In other words, a robot has *sensors* to monitor the environment, *processors* to make decisions as to how to react to the environment (thus incorporating some degree of programmability or artificial intelligence), and *actuators* to

[62] Schmitt, 'Classification' (n 58) 256; *Tallinn Manual* (n 20) commentary to r 23, ¶ 15.

[63] See Schmitt, 'Classification' (n 58) 256; *Tallinn Manual* (n 20) commentary to r 23, ¶¶ 13, 15; for an analysis of different scenarios pertaining to the level of organisation, see Roscini (n 19) 155–157.

[64] *AP Commentary* ¶ 4470.

[65] *Prosecutor v Bemba (Decision on the Confirmation of Charges)* (Case no ICC-01/05-01/08, ICC Pre-Trial Chamber III, 15 June 2009) ¶234.

[66] *Tallinn Manual* (n 20) commentary to r 23, ¶ 14, n 202.

[67] See *Prosecutor v Boskoski* (ICTY-04-82-T, ICTY Judgment, 10 July 2008) ¶ 205.

[68] See *Tallinn Manual* (n 20) commentary to r 23, ¶ 7.

[69] Bruno Siciliano and Oussama Khatib, 'Introduction' in Bruno Siciliano and Oussama Khatib (eds), *Springer Handbook of Robotics* (Springer 2008) 1, 1.

[70] Alan Winfield, *Robotics: A Very Short Introduction* (OUP 2012) 8–9.

effect change in the environment.[71] What remains controversial, however, is whether a device must have some meaningful degree of autonomy in order to be deemed a robot.[72] Autonomy, in this context, refers to the capacity of the device to undertake some action without intervention from a human operator.[73]

While it is important to appreciate that different devices have different levels of autonomy with respect to each of their functions – being autonomous is a matter of degree[74] – it does not appear to be easy, nor particularly helpful in this context, to try to establish a requisite minimal degree of autonomy for something to be called a 'robot'. The field of 'robotics' and the notion of 'robotic technology' are broad enough to cover sophisticated electromechanical systems that rely heavily on a sensing–processing–acting loop but have very limited autonomy. For example, the area of telerobotics deals with devices where high-level cognitive decisions are made by a human operator while the device is responsible for the mechanical implementation of these decisions some distance away.[75] There is, however, very little autonomy involved. For the purposes of this discussion, we take the widest possible view of robotics: we believe that utilising narrow definitions has the potential of ignoring how devices with a greater degree of autonomy are essentially incremental developments of less-sophisticated devices.

Especially in view of a broad definition of the term, military applications of robotics are numerous. One commonplace example is the use of fly-by-wire (FBW) technology on military aircraft. With a FBW system, the connection between the cockpit controls (such as the yoke or joystick, and rudder pedals) on the one hand, and the flight control surfaces and engines on the other hand, is electronic rather than mechanical.[76] Essentially the same concept is used in many remotely controlled weapons stations (RCWS) – systems controlled by operators who are not in direct (physical) contact with the weapons. For example, a gun turret may be mounted on a vehicle and be controlled by an operator inside. Such systems

---

[71] Cf P W Singer, *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century* (Penguin 2009) 67; Armin Krishnan, *Killer Robots: Legality and Ethicality of Autonomous Weapons* (Ashgate 2009) 9.

[72] Cf US Department of Defence, *Joint Robotics Program Master Plan FY2005* (2005) 1–2 (suggesting that a robot 'works automatically or operates by remote control'); Krishnan (n 71) 9 ('A robot must exhibit some degree of autonomy, even if it is only very limited autonomy.').

[73] See Winfield (n 70) 10.

[74] See, notably, Thomas B Sheridan and William L Verplank, 'Human and Computer Control of Undersea Teleoperators', Technical Report (Massachusetts Institute of Technology, 14 July 1978).

[75] See, eg, Günter Niemeyer, Carsten Preusche and Gerd Hirzinger, 'Telerobotics' in Bruno Siciliano and Oussama Khatib (eds), *Springer Handbook of Robotics* (Springer 2008) 741, 741.

[76] See, eg, Nick Lee-Frampton, 'Anything but Simple: The F-16's FBW Flight Control System' (January/February 2000) 54(9) *New Zealand Engineering* 13.

are widely used both on land, for example on armoured fighting vehicles,[77] as well as on naval vessels.[78]

The rapidly increasing ability to combine robotics with sophisticated sensing systems (radars, electro-optical and infrared sensors) and a communication link has paved the way for advanced remotely controlled military systems. Remotely piloted vehicles (RPVs) are now available in all traditional domains of warfare – land, sea and air.[79] Remotely piloted aircraft (RPAs) – also called unmanned aerial vehicles (UAVs) or, popularly, 'drones' – are used widely for intelligence, surveillance and reconnaissance purposes. According to a 2013 report, '[b]oth military and civilian UAVs are in use by almost every country, including nearly 60 with their own manufacturing capability'.[80] RPAs carrying weapons, on the other hand, have remained the purview of a considerably smaller number of states: a 2014 report identified 23 states as potentially developing some type of armed RPAs.[81] Thus, much of the prominence of RPVs has to do with their extensive use by the US: between 2002 and early 2015, it had carried out more than 500 strikes using RPAs, with the greatest number in Pakistan.[82]

Military systems are obtaining an increasing degree of autonomy in relation to some of their functions.[83] For example, some RPAs currently in operation, such as the RQ-4 Global Hawk, have a considerable ability to navigate on a pre-defined flight plan without any human intervention. The Northrop Grumman X-47B, a strike fighter-sized RPV prototype, has demonstrated the feasibility of unsupervised aerial refuelling.[84] Certain weapon systems are also capable of operation without continuous control by an operator. Notable examples include 'close-in weapon systems' (CIWS) on naval vessels, and their land-based counterparts, C-RAMs (short for 'counter rocket, artillery and mortar'). In a nutshell, CIWS

[77] See, eg, Ezio Bonsignore and David Eshel, 'Remotely Controlled Weapon Stations: Technologies and Markets' (2009) 33(7) *Military Technology* 52.

[78] See, eg, Luca Peruzzi, 'Remote Control Cannon Proliferation at Sea' (2013) 37(4) *Armada International* 26.

[79] For an overview of the technology, see, eg, US Department of Defense, 'Unmanned Systems Integrated Roadmap FY2013–2038', Ref No 14-S-0553 (2013).

[80] 'UAV Roundup 2013' (July–August 2013) *Aerospace America* 26, 26; see also Lynn E Davis et al, *Armed and Dangerous? UAVs and U.S. Security* (RAND 2014).

[81] Davis (n 80) 7.

[82] The Bureau of Investigative Journalism, 'Get the Data: Drone Wars' <https://www.thebureauinvestigates.com/category/projects/drones/drones-graphs>.

[83] As the US Defense Science Board has noted, '[a]utonomy is better understood as a capability (or a set of capabilities) that enables the larger human-machine system to accomplish a given mission, rather than as a "black box" that can be discussed separately from the vehicle and the mission'. US Defense Science Board, 'Task Force Report: The Role of Autonomy in DoD Systems' (July 2012) 21 <http://fas.org/irp/agency/dod/dsb/autonomy.pdf >.

[84] See 'Fueled in flight: X-47B first to complete autonomous aerial refueling', *NAVAIR News* (22 April 2015) <http://www.navair.navy.mil/index.cfm?fuseaction=home.NAVAIRNewsStory&id=5880>.

and C-RAM are rapid-fire, computer-controlled, radar-guided guns designed to automatically engage and defeat incoming missiles and other close-in threats.[85]

2.2 Legal challenges

Philip Alston, the UN Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, noted in a 2010 report that

> [a]lthough robotic or unmanned weapons technology has developed at astonishing rates, the public debate over the legal, ethical and moral issues arising from its use is at a very early stage, and very little consideration has been given to the international legal framework necessary for dealing with the resulting issues.[86]

The widely-reported and often contentious use of RPAs for 'targeted killings' has, however, fuelled an intense debate about the legality and morality of remotely controlled weapons.[87]

The single most controversial international law issue in this regards has been the determination of the appropriate regulatory framework. The use of violence in the course of an armed conflict is subject to the restrictions of LOAC. This framework is relatively permissive: in particular, it accepts the lethal targeting of persons on the basis of their status (combatants) or their conduct (direct participation in hostilities), and tolerates civilian deaths insofar as they are incidental to an attack against a legitimate military objective and proportionate to the military advantage gained from the attack.[88] Use of armed force outside an armed conflict, on the other hand, is governed by the fairly restrictive human rights law. Under human rights standards, a state may use lethal force only where 'it is required to protect life … and there is no other means, such as capture or non-lethal incapacitation, of preventing that threat to life …'.[89]

---

[85] See, eg, Raytheon, 'Phalanx Close-In Weapon System: Last Line of Defense for air, land and sea' <http://www.raytheon.com/capabilities/products/phalanx>.

[86] Philip Alston (Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions), Interim Report to the General Assembly, UN Doc A/65/32 (23 August 2010) para 29.

[87] See, eg, PW Singer, *Wired For War: The Robotics Revolution and Conflict in the 21st Century* (Penguin 2009); Claire Finkelstein, Jens David Ohlin and Andrew Altman (eds), *Targeted Killings: Law and Morality in an Asymmetrical World* (OUP 2012); Bradley Jay Strawser (ed), *Killing by Remote Control: The Ethics of an Unmanned Military* (OUP 2013); Christian Enemark, *Armed Drones and the Ethics of War: Military Virtue in a Post-Heroic Age* (Routledge 2014); John Kaag and Sarah Kreps, *Drone Warfare* (Polity 2014); Special Issue: Unmanned Vehicles, Legal, Social and Ethical Issues (2012) 21(2) *JLIS*; Special Issue: Legal and Ethical Implications of Drone Warfare (2015) 19(2) *International Journal of Human Rights* 105.

[88] See generally, pt II of this volume.

[89] Philip Alston (Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions), Report to the Human Rights Council, Addendum: Study on Targeted Killings, UN Doc A/HRC/14/24/Add.6 (28 May 2010) para 32.

Given the disparity of these standards, the lawfulness of a particular RPV attack would heavily depend on whether LOAC is applicable. The initial issue in this respect is the existence of an armed conflict that would trigger the application of LOAC.[90] But even when there is an armed conflict, LOAC would apply to hostilities in the context of that armed conflict. Hence, to apply LOAC to a specific attack, there must be a connection between that attack and the armed conflict. This issue has become particularly problematic in relation to US RPA strikes against al-Qaeda in Pakistan: it is unclear whether these can be seen as occurring in the context of an armed conflict, such as the non-international armed conflict against al-Qaeda in Afghanistan.[91]

Where LOAC is applicable, it is doubtful whether remotely controlled weapon systems pose, in and of themselves, any novel issues in terms of rules governing the conduct of hostilities. Weapon-specific rules place no restriction on the development, acquisition or use of weapons that are controlled remotely.[92] Of course, no weapon can be placed lawfully on an RPV that could not be placed lawfully on a manned vehicle. Thus, for example, a state party to the 2008 Convention on Cluster Munitions [93] would be precluded from arming its RPVs with cluster munitions.

Complying with the principles of discrimination and proportionality, and taking precautionary measures, does not appear to be more difficult when launching an attack by means of a weapon carried by a RPV as compared to a comparable manned vehicle. To the contrary, in some circumstances RPVs may enhance compliance with LOAC. Removing the operator from immediate danger and making use of the advanced sensing capabilities of RPVs may allow for more thoroughly considered and accurate targeting decisions.[94] Paradoxically, LOAC may thus encourage the use of RPVs.[95]

An oft-expressed concern in relation to RPVs has to do with the status of their operators under LOAC. While difficulties in classifying persons for the purposes of LOAC are hardly a problem specific to this operational context,[96] it is certainly true that civilian operators of remotely controlled systems can easily become direct participants in hostilities, with all the

---

[90] See generally Dwyer and McCormack (n 57).

[91] See, eg, Chris Jenks, 'Law from Above: Unmanned Aerial Systems, Use of Force, and the Law of Armed Conflict' (2010) 85 *North Dakota Law Review* 649; Ian Henderson and Bryan Cavanagh, 'Unmanned Aerial Vehicles: Do They Pose Legal Challenges?' in Nasu and McLaughlin (eds) (n 5) 193, 200–201.

[92] See, eg, Meredith Hagger and Tim McCormack, 'Regulating the Use of Unmanned Combat Vehicles: Are General Principles of International Humanitarian Law Sufficient?' (2011) 21 *JLIS* 74, 84–85.

[93] (3 December 2008) 2688 UNTS 39.

[94] Cf Jenks (n 91) 668–669; Henderson and Cavanagh (n 91) 205–206.

[95] See Michael W Lewis and Emily Crawford, 'Drones and Distinction: How IHL Encouraged the Rise of Drones' (2013) 44 *Georgetown Journal of International Law* 1127.

[96] See, eg, Nelleke van Amstel and Rain Liivoja, 'Private Military and Security Companies', ch 37 of this volume, s 2 (in relation to employees of private companies).

attendant consequences.[97] This would be the case not only where a remote operator, say, launches an attack from an RPV, but also where the operator of an unarmed RPV passes information about the location of adversary military forces to ground troops for the purposes of launching a land-based attack.

Additional legal and ethical issues arise from the increased autonomy of military systems, which has already generated quite a voluminous body of literature.[98] Broad questions as to the safety of a system will arise from any kind of operation where a human is not in control, such as the unsupervised flight of a UAV along a predetermined flight path – notwithstanding that human-controlled operation might not, on the evidence, be any safer. [99] But a weapon system that can identify targets and launch attacks upon them without attack-specific human oversight generates significant issues under LOAC.

International law does not specifically restrict the degree of autonomy that can be implemented in weapon systems. Thus the key problem is whether the weapon system is capable of operating in compliance with LOAC, in particular: Can the system adequately distinguish between combatants and civilians, and military objectives and civilian objects? Can the system assess collateral damage? Can the system recognise surrender?

Arguably these are primarily technical challenges, potentially capable of a technical solution, rather than legal problems requiring a regulatory remedy.[100] In any event, one should not assume that any autonomous systems would have to be given the same amount of discretion as a soldier, only to find that the system is incapable of exercising that discretion in conformity with LOAC (especially, assessing the maximum permissible collateral damage). The LOAC compliance of a particular system may be ensured by programming it to identify a very narrow range of objects that by their clearly identifiable nature or behaviour are military objectives (say, submarines or incoming missiles) and to deploy them only where no civilians or civilian objects can be identified in the vicinity. This may well be

[97] See API arts 51(3); APII art 13(3); Lesh (n 88).

[98] See, eg, Patrick Lin, George Bekey and Keith Abney, 'Autonomous Military Robotics: Risk, Ethics, and Design' (Ethics + Emerging Sciences Group, California Polytechnic State University, 20 December 2008); Ronald C Arkin, *Governing Lethal Behaviour in Autonomous Robots* (CRC Press 2009); Armin Krishnan, *Killer Robots: Legality and Ethicality of Autonomous Weapons* (Ashgate 2009); Jai Galliott, *Military Robots: Mapping the Moral Landscape* (Ashgate 2015); 'Autonomous weapon systems: technical, military, legal and humanitarian aspects', Report of the ICRC Expert Meeting, Geneva 26-28 March 2014 (9 May 2014) < https://www.icrc.org/eng/assets/files/2014/expert-meeting-autonomous-weapons-icrc-report-2014-05-09.pdf>.

[99] See Chris Jenks, 'False Rubicons, Human Placebos and Increasingly Autonomous Weapon Systems' (forthcoming).

[100] On the distinction, see Tim McFarland, 'How Should Lawyers Think about Weapon Autonomy?' forthcoming in (2015) *IRRC.*

easier to achieve in some operational settings, such as remote deserts, open oceans and depopulated areas.[101]

Significant legal issues do arise in terms of accountability. In autonomous systems, certain decisions normally made by humans are 'delegated' to the system such that the need for input from a human operator is reduced and the operation of the system is determined by computer software. [102] Yet it would be fanciful to think that the system thereby becomes an accountable agent and human beings are removed from the decision-making process; rather, the nature of the decisions made by humans changes: such decisions will be more general, made ahead of deployment and involve greater degree of forecasting.[103] To put it differently, an autonomous system will have been designed, built, programmed, approved and deployed by people, who will ultimately remain responsible for the 'conduct' of the system. Admittedly, allocating that responsibility between those human actors may be a difficult enterprise. Part of this difficulty results from the assumption underlying LOAC and international criminal law that the operator of a weapon system has ultimate control over it. With autonomous – or, for that matter, other highly advanced – systems that would not necessarily be the case: the designer and programmer could have more control over a system than the person switching it on. Current modes of individual criminal responsibility might not be adequate to reflect this new reality.[104]

Finally, RPVs or autonomous systems can potentially affect other areas of LOAC, for example, the law of occupation. Under LOAC, a territory is considered occupied when it falls under the actual control of the adversary.[105] Traditionally, this has meant 'boots on the ground' – the presence of military personnel exercising authority in the territory. Technology can undoubtedly allow certain kinds of military operations to be carried out without such presence of personnel. This raises the question whether the control potentially exercisable through a combination of RPVs and autonomous systems can be such as to warrant a reinterpretation of certain basic tenets of the law of occupation

[101] See William H Boothby, *Conflict Law: The Influence of New Weapons Technology, Human Rights and Emerging Actors* (Asser 2014) 111.

[102] Cf ibid 105 ('The significant element of autonomy is the ability of the system to decide a course of action from a number of alternatives without depending on human oversight and control.').

[103] See McFarland (n 100).

[104] See Tim McCormack and Tim McFarland, 'Mind the Gap: Can Developers of Autonomous Weapons Systems be Liable for War Crimes?' (2014) 90 *International Law Studies* 361.

[105] HR article 42.

3 Nanotechnology

3.1 Technology

Nanotechnology – conceptualised in the late 1950s, and introduced to a wider audience in the 1970s and 1980s[106] – refers to 'technology at the nanoscale'.[107] The broad term 'technology' includes applications from just about every field of science. Nanoscale, for its part, refers to the size of these applications, and covers a range of 1 to 100 nanometres.[108] (A nanometre is one billionth of a metre – a factor of 10^{-9}. To put this in perspective, a nanometre is to a metre what a marble is to the size of the Earth.[109]) Thus, nanotechnology involves the deliberate manipulation of material on the atomic or molecular level to produce novel materials, devices and systems.[110]

Much of nanotechnology is concerned with nanomaterials, that is to say materials that have one or more dimensions on the nanoscale.[111] The most common type of these materials, a nanoparticle, has all three dimensions on the nanoscale.[112] Nanoparticles occur naturally in the environment, such as in volcanic ash, sea spray, clay, and milk, and in some man-made substances, such as depleted uranium. In the field of nanotechnology, however, scientists and engineers have an increasingly sophisticated ability to manipulate, design and develop novel nanoparticles.

Chemicals at the nanoparticle size behave differently to chemicals at 'normal size'. They may be more conductive, have stronger bonds, or be more chemically reactive than larger particles of the same substance. For example, gold, chemically inert at normal size, can serve as a chemical catalyst at the nanoscale.[113] Furthermore, surface charge – the potential

---

[106] See, especially, Richard Feynman, 'Plenty of Room at the Bottom' (Talk given to the American Physical Society, Pasadena, December 1959) <http://www.pa.msu.edu/~yang/RFeynman_plentySpace.pdf>; K Eric Drexler, *Engines of Creation: The Coming Era of Nanotechnology* (Anchor 1986).

[107] Jeremy Ramsden, *Nanotechnology: An Introduction* (Elsevier 2011) 2.

[108] ibid.

[109] Jennifer Kahn, 'Nanotechnology', *National Geographic* (June 2006) 98.

[110] For definitions along these lines, see, eg, Interagency Working Group on Nanoscience, Engineering and Technology, 'National Nanotechnology Initiative: Leading to the Next Industrial Revolution' (Committee on Technology, National Science and Technology Council, February 2000) 15; The Foresight Institute, 'About Nanotechnology' <https://www.foresight.org/nano>.

[111] Ramsden (n 107) 101–103.

[112] ibid.

[113] See, eg, Naomi Lubick and Kellyn Betts, 'Silver Socks Have Cloudy Lining: Court Bans Widely Used Flame Retardant' (2008) 42 *Environmental Science & Technology* 3910.

electrical energy between the particle surface and the medium in which it moves[114] – appears to play a greater role at the nanoscale.

As a consequence, substances made of or incorporating nanoparticles may have markedly different, and often enhanced, mechanical, catalytic and thermal properties. Nanoparticles can be utilised, for example, to create more resistant surfaces and to produce active filters to protect against toxic chemical and biological threats. Also, nanotechnology 'helps to enhance specific biological reactions as drug delivery systems help to pass through biological barriers',[115] leading to*, inter alia,* more efficient (targeted) drug delivery, and creating new opportunities for cell imaging.

What are often referred to as 'nanorobots' are effectively assemblies of atoms that have the ability to trap, transport and alter other atoms. They are 'programmable, potentially self-replicating, molecular machines made of specifically arranged atoms'.[116] Scientists working on this cutting-edge research describe their beneficent vision of a future in which 'nanorobots' would 'cruise around inside the body, communicating with each other and performing various kinds of diagnoses and therapy'.[117] The possibility of using 'nanorobots' to seek out specific organs, and even specific cells, opens up opens up new approaches to much less invasive, highly targeted and hence more effective administration of drugs or of micro-surgical techniques.

As this brief discussion indicates, the applications for nanotechnology are many and they span, *inter alia*, biotechnology, medicine, microelectronics, energy conversion and storage, coatings, textiles, pharmaceuticals, cosmetics, food, manufacturing and security. Many of these applications are already exploited in a wide range of commercial products.[118] For example, gold nanoparticles, mentioned earlier, are used in biosensors, cancer cell imaging and drug delivery to cell membranes.[119]

In the same way that other areas of science and technology can be dual-purpose, there is little doubt that nanotechnology may also be repurposed in a military context: the distinct

---

[114] See International Union of Pure and Applied Chemistry, *Compendium of Chemical Terminology* (2nd ed, Blackwell Scientific Publications 1997).

[115] Johann Ach and Beate Luttenberg (eds), *Nanobiotechnology, Nanomedicine and Human Enhancement* (Lit 2008).

[116] Jun Wang and Peter J Dortmans, 'A Review of Selected Nanotechnology Topics and Their Potential Military Applications', Report no DSTO-TN-0537 (DSTO Systems Sciences Laboratory 2004) 4.

[117] Kristna Weidner,'Nanomotors are controlled for the first time, within living cells', *Penn State News* (11 February 2014) <http://news.psu.edu/story/303296/2014/02/10/research/nanomotors-are-controlled-first-time-inside-living-cells>.

[118] Maxine McCall, 'Nanoparticles and Nanosafety: The Big Picture', *The Conversation* (6 February 2014) <http://theconversation.com/nanoparticles-and-nanosafety-the-big-picture-22061>.

[119] Madhusudhan R Papasani, Guankui Wang and Rodney A Hill, 'Gold Nanoparticles: The Importance of Physiological Principles to Devise Strategies for Targeted Drug Delivery (2012) 8(6) *Nanomedicine: Nanotechnology, Biology and Medicine* 804.

properties of materials at the nanoscale offer new potential applications for armed conflict. The potential military uses of nanotechnology – both offensive and defensive – have been explored in the literature, although not exhaustively.[120] A notable difficulty in this respect is the futuristic, and sometimes classified, nature of research in this area, which means that potential military nanotechnology applications and estimates of development time frames have to be extrapolated from present science and technology.[121]

While many potential military applications of nanotechnology remain speculative, it is possible to give a few illustrations. The unique properties of matter observed at the nanoscale have been utilised to improve sensors,[122] to enhance protective vests worn by military and para-military personnel,[123] as well as to develop new types of armour and communication equipment.[124] Nano-enhanced energy storage is being developed with implications for fuel cells, soldier systems, small robots, RPVs, and outer space technology.[125] Nanotechnology may improve the penetration capability and accuracy of projectiles, and enhance camouflaging.[126] Furthermore, given its therapeutic potential, nanotechnology could also 'facilitate weapons based on enhanced delivery mechanisms for toxic substances, on tailored compounds capable of targeting specific physiological functions, and on complex multi-layered stealth designs.'[127]

3.2 Legal challenges

Since nanotechnology includes manipulation of chemical and biological functions, specific rules which govern chemical and biological weapons may have relevance where nanotechnology is used in the military context, even though no nanotechnology-derived weapons appear to be in production as yet. In the chemical and biological warfare context, there are at least four broad areas where nanotechnology has regulatory implications: (1) nano-ena-

[120] See, in particular, Wang and Dortmans (n 116); Jürgen Altmann, *Military Nanotechnology* (Routledge 2006); Margaret Kosal, *Nanotechnology for Chemical and Biological Defense* (Springer 2009); Wilson Wong, *Emerging Military Technologies: A Guide to the Issues* (Praeger 2013) ch 5.

[121] Altmann (n 120) 71.

[122] Margaret Kosal, 'The Security Implications of Nanotechnology' (2013) 66 *Bulletin of the Atomic Scientists* 58.

[123] See, eg, Kanesalingam Sinnppoo, Lyndon Arnold and Rajiv Padhye, 'Application of Wool in High-velocity Ballistic Protective Fabrics' (2010) 80 *Textile Research Journal* 1083.

[124] Wang and Dortmans (n 116).

[125] Altmann (n 120) 78-79.

[126] Thomas Faunce and Hitoshi Nasu, 'Nanotechnology and the International Law of Weaponry: Towards International Regulation of Nano-Weapons' (2010) 20 *JLIS* 21; Hitoshi Nasu, 'Nanotechnology and Challenges to International Humanitarian Law: A Preliminary Legal Assessment' (2012) 94(886) *IRRC* 653.

[127] Juan Pardo-Guerra and Francisco Aguayo Ayala, 'Nanotechnology and the International Regime on Chemical and Biological Weapons' (2005) 2 *Law and Business* 1.

bled delivery methods, (2) novel nanotechnology-based biochemical weapons, (3) nanoparticles and nanomaterials with toxicological or deleterious health properties, and (4) nanotechnology-enabled evasion of medical countermeasures.[128]

The 1925 Geneva Protocol prohibits the use of 'asphyxiating, poisonous or other gases, and of all analogous liquids, materials or devices' and 'bacteriological methods of warfare'.[129] This prohibition is extended by the 1972 Biological Weapons Convention (BWC) and the 1993 Chemical Weapons Convention (CWC) to cover the development, production, acquisition, stockpiling and transfer of biological and chemical weapons respectively.[130] The creation of synthetic DNA has effectively increased the 'continuous biochemical threat spectrum' with the BWC and CWC prohibitions 'overlapping in their coverage of mid-spectrum agents such as toxins and bioregulators'.[131]

To determine their scope of application, the BWC and CWC use broad terms such as 'microbial or other biological agents', 'toxins' and 'toxic chemicals',[132] making the conventions applicable to any new technologies that involve chemical or biological agents used for hostile purposes. The conventions, and the corresponding rules of customary international law, remain applicable regardless of the size of the matter in question.

That said, the BWC is concerned with living organisms and substances produced by such organisms. It has been suggested that artificially created nanoparticles or 'nanorobots' fall within the scope of the BWC prohibition if they replicate the behaviour of known biological agents.[133] On the other hand, nanoparticles that interact with their host through their chemical action on life processes fall squarely under the prohibition contained in the CWC, regardless of their size.[134]

Significantly, however, the prohibition of biological weapons extends to 'equipment or means of delivery designed to use such [biological] agents or toxins for hostile purposes or in armed conflict' and the definition of chemical weapons expressly includes 'munitions

---

[128] Kosal, *Chemical and Biological Defence* (n 120) ch 4.

[129] Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare (17 June 1925) 94 LNTS 65.

[130] Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction (10 April 1972) 1015 UNTS 163, arts 1 and 3; Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (13 January 1993) 1974 UNTS 45, art 1.

[131] Mark Wheelis and Malcolm Dando, 'Neurobiology: A Case Study for the Imminent Militarization of Biology' (2005) 87(859) *IRRC* 560; see also

[132] BWC art 1(1); CWC art 2(2).

[133] Robert Pinson, 'Is Nanotechnology Prohibited by the Biological and Chemical Weapons Conventions?' (2004) 22 *Berkeley Journal of International Law* 279, 298–300.

[134] ibid 300–304.

and devices' for the release of toxic chemicals.[135] This would also capture any nano-technological means of delivering biological agents or toxic chemicals into the human body.

Nanoscale objects can, however, affect human physiology by way of their physical properties rather than by their chemical composition. For example, the inhalation of silver nanofibers has been shown to cause an acute inflammatory reaction in the lungs, with the severity of reaction dependant on the length of the fibre.[136] Also, an accumulation of nanoparticles in the human body – for example the build-up of nanogold, used as an anti-inflammatory agent for conditions such as arthritis[137] – could be manipulated externally (i.e. heated) to cause damage to the human body. Finally, 'nanorobots' could potentially be programmed to cause mechanical injury at the cellular level without any biochemical action. The absence of a toxic chemical or disease-causing organism in these instances suggests that the prohibitions contained in the BWC and CWC could be inapplicable. Arguably, however, the broad customary law prohibition of poisoning, codified in the Hague Regulations,[138] would prohibit such uses of nanotechnology.[139] Also, causing tissue damage by means of nanoparticles or 'nanorobots' that due to their size or other properties cannot be detected by industry-standard medical imaging devices may run afoul of the ban on 'any weapon the primary effect of which is to injure by fragments which in the human body escape detection by X-rays'.[140]

Rules and principles on the protection of the environment may also play a role in the use and application of nanotechnology for military purposes. The ENMOD Convention prohibits the 'military or any other hostile use of environmental modification techniques having widespread, long-lasting or severe effects as the means of destruction, damage or injury to any other State Party'[141] and Additional Protocol I bans methods or means of warfare 'which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment'.[142] While the precise environmental impact of engineered nanomaterials and nanoparticles remains unclear, there is evidence that at least some of them pose significant risks to the natural environment.[143] This raises the question whether

[135] BWC art 1(2); CWC art 2(1)(b)–(c).

[136] Anja Schinwald et al, 'The Threshold Length for Fibre-Induced Acute Pleural Inflammation: Shedding Light on the Early Events in Asbestos-Induced Mesothelioma' (2012) 128(2) *Toxicological Sciences* 461.

[137] Christine T N Pham, 'Nanotherapeutic Approaches for the Treatment of Rheumatoid Arthritis' (2011) 3 *Wiley Interdisciplinary Reviews: Nanomedicine and Nanobiotechnology* 607.

[138] HR art 23(a).

[139] On the scope of the prohibition on the use of poison and poisoned weapons, see Robert J Mathews, 'Chemical and Biological Weapons', ch 2 in this volume, in particular section 1.

[140] Protocol (I) on Non-Detectable Fragments (10 October 1980) 1342 UNTS 168.

[141] Convention on the Prohibition of Military or any Other Hostile Use of Environmental Modification Techniques, Geneva, 2 September 1976, Article I

[142] API art 35(3).

[143] See Hitoshi Nasu, 'Nanotechnology and Challenges to International Humanitarian Law: A Preliminary Legal Assessment' (2012) 94 *IRRC* 653, 655–656 and the sources cited therein.

the precautionary principle recognised in environmental law applies equally during times of armed conflict.[144]

4 Weapons review

Article 36 of Additional Protocol I provides an obligation to conduct due diligence in relation to some military applications of technology:

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

Even though this provision is contained in Additional Protocol I that is applicable in armed conflict, the effect of Article 36 is such that legal review needs to be undertaken irrespective of whether the state in question is involved in an armed conflict.

Article 36 is broad in scope. In terms of the object of review, it refers to any 'new weapon, means and method of warfare'. This clearly covers, for example, novel projectiles as well as innovative devices for propelling them. The reference to methods of warfare also subjects to legal review military technology that, despite not being directly used to harm the adversary, nonetheless changes the way in which hostilities are undertaken. Thus, for instance, armed RPVs, even if they carry previously known and reviewed weapons, may become new means or methods of warfare and thus subject to a legal review.

Article 36 is also extensive in terms of the relevant legal framework. The review obligation extends well beyond the rules contained in Additional Protocol I itself. The phrase 'any other rule of international law applicable to the High Contracting Party' clearly refers to other LOAC treaties as well as customary international law.[145] Moreover, the ICRC *Commentary* makes it plain that the phrase also 'refers to any agreement on disarmament concluded by the Party concerned, or any other agreement related to the prohibition, limitation or restriction on the use of a weapon or a particular type of weapon, concluded by this Party'.[146] The broad language of Article 36 suggests that the compatibility of weapons, means and methods of warfare with applicable human rights law or environmental law obligations must also be assessed, to the extent that those branches of international law apply in armed conflict.

The broad scope of Article 36 and the complexity of new military platforms can make the legal review of new weapons, means and methods a difficult task. Weapons' reviewers must not only have a thorough knowledge of the applicable law, they must also have an understanding of the 'engineering design, production and testing (or validation) methods,

---

[144] See Laurent Hourcle, 'Environmental Law of War' (2001) 25 *Vermont LR* 653.

[145] *AP Commentary* para 1472.

[146] ibid.

and the way in which the weapon might be employed on the battlefield'.[147] Thus, the obligation under Article 36 necessitates close collaboration between scientists, engineers and lawyers so as to ensure compliance with the requirement to review weapons. Also, given the immediate military applications of some advances in technology, Article 36 reviews may need to be conducted earlier in the development process than previously.

Unfortunately, Article 36 suffers from a striking lack of national implementation. Only a handful of states parties to Additional Protocol I, and two non-parties (the US and Israel), have in place procedures for systematically conducting reviews of new weapons, means and methods of warfare. Even when such reviews are conducted, they do not necessarily reveal all of the relevant legal issues: as pointed out earlier, some emerging technologies raise legal difficulties not in relation to specific prohibitions or restrictions arising under LOAC, arms control law or even human rights law, but because they challenge some of the assumptions that underlie these legal regimes (for example, what constitutes 'attack' or how accountability with respect to systems with a degree of autonomy is implemented). Thus, while a more diligent national application of Article 36 should certainly be welcomed, even broader legal reviews may be necessary for some types of emerging technology.

5 Concluding remarks

Rapid technological developments in the defence sector have justifiably caused concern, especially within civil society and among scholars. This has led to calls for additional regulation. It has been suggested that '[t]he world needs a Geneva Convention for cybercombat'.[148] It has been argued that states should 'control and regulate the proliferation of drones through the judicious use of international law'[149] and that they 'should prohibit the creation of weapons that have full autonomy to decide when to apply lethal force'.[150] It has been claimed that and that 'there is an urgent need for regulating nano-weapons under the international law of weaponry'[151] and that '[p]ast methods for other technologies are not adequate to deal with nanotechnology'[152] such that reducing the risk of misuse requires both '[t]raditional and innovative new approaches to non-proliferation and counterproliferation'.[153] In short, there appears to be a growing sentiment in some quarters that the existing law is inadequate. Many LOAC specialists, on the other hand, tend to be more optimistic.

---

[147] Alan Backstrom and Ian Henderson, 'New Capabilities in Warfare: An Overview of Contemporary Technological Developments and the Associated Legal and Engineering Issues in Article 36 Weapons Reviews' (2012) 94(886) *IRRC* 483, 484.

[148] Karl Rauscher, 'It's Time to Write the Rules of Cyberwar', IEEE Spectrum (27 November 2013) <http://spectrum.ieee.org/telecom/security/its-time-to-write-the-rules-of-cyberwar>.

[149] Kaag and Kreps (n 87) 151; Sarah Kreps and Micah Zenko, 'The Next Drone Wars: Preparing for Proliferation' (2014) 93(2) *Foreign Affairs* 68.

[150] Human Rights Watch, *Losing Humanity: The Case against Killer Robots* (2012) 46.

[151] Faunce and Nasu (n 126) 59; see also Altmann (n 120).

[152] Kosal, 'Security Implications' (n 122) 59.

[153] Kosal, *Chemical and Biological Defence* (n 120) 8.

One commentator concludes that, at least with respect to targeting rules, 'the existing body of law is capable of being applied to novel weapons technologies'.[154]

We take an intermediate position. We believe that much of LOAC is flexible enough to be applied to any weapon technology that might be fielded. That said, some of the current scientific and technological developments do point to weaknesses or uncertainties in the law. Some of these problems could, however, be overcome by more up-to-date interpretations of the current law, rather than the adoption of new, ever-more intricate rules. For instance, in the context of cyber operations, revisiting the meaning of the term 'damage' would help clarify some of the uncertainties. A major difficulty, however, is that the use of emerging technologies – including specifically cyber capabilities and RPVs – constitutes an area where states have been exceedingly reluctant to clearly express their legal views.[155] We share the concern that this unwillingness to express *opinio juris* will have detrimental effects on the development of LOAC.[156]

Finally, it is worth keeping in mind that efforts to ban outright military applications of particular kinds of technology may have unintended consequences: unqualified restrictions, however well-intentioned, can prove to be counter-humanitarian. As regards autonomous systems, for example, it is worth recalling the 1988 incident where the US missile cruiser *USS Vincennes* shot down an Iranian civilian airliner, mistaking it for an attacking military fighter. The disaster could have been avoided, however, had the commander of the *Vincennes* relied on the data supplied by the Aegis Combat System, which was consistent with a civilian aircraft. This suggests that, at least in some situations, an autonomous system would react more appropriately to potential threats than a combatant. RPVs and nanotechnology serve as illustrations of dual-use technology, the regulation of which has its inherent challenges. Any restriction of the use of such technology would need to accommodate the research and development of beneficial (civilian) applications.

[154] William H Boothby, 'Legal Challenges of New Technologies: An Overview' in Nasu and McLaughlin (eds) (n 5) 21, 25. Boothby concedes, though that 'if novel technology should emerge which raises humanitarian concerns that cannot easily be addressed by the application of existing law, it would be for the international community of states decide whether new, specific treaty regulation is required to address such concerns.' ibid.

[155] See Michael N Schmitt and Sean Watts, 'The Decline of International Humanitarian Law: *Opinio Juris* and the Law of Cyber Warfare' (2015) 50 *Texas International Law Journal* 189.

[156] ibid.