European Journal of International Security, Vol. 1, part 1, pp. 94–111. doi:10.1017/eis.2015.7

EJIS

Future arms, technologies, and international law: Preventive security governance

Denise Garcia*

Sadeleer Research Faculty & Associate Professor, Department of Political Science and International Affairs Programme, Northeastern University

Abstract

This article presents an initial discussion of the political and legal challenges associated with weaponised technologies in three interconnected areas that may impinge upon the ability to protect civilian populations during peace and war and imperil international security: armed unmanned combat aerial vehicles (commonly known as drones); autonomous weapons systems (known as 'killer robots'); and the potential militarisation of cyberspace, or its use as a weapon, and the operation of drones and killer robots in the cyber domain. Supporting the argument that the world is 'facing new methods of warfare' and that international security governance and law are not keeping up, the article provides an overview and interpretation of three technologies in connection with aspects of five branches of law: state responsibility, use of force, international humanitarian law, human rights law, and law of the commons. I argue therefore that 'preventive security governance' could be a strategy to curtail uncertainty in the preservation of stability and international order. I define 'preventive security governance' as the codification of specific or new global norms, arising from existing international law that will clarify expectations and universally agreed behaviour on a given issue-area. This is essential for a peaceful future for humanity and for international order and stability.

Keywords

Autonomous Weapons Systems; Killer Robots; Cyber Warfare; International Norms; Preventive Security Governance

Introduction

The world is facing new potentially destructive means and methods of warfare, and it is not yet clear how international law will apply to such emerging threats or whether existing global security governance structures will be sufficient. The capacity to launch cyber attacks, the use of remotely-controlled armed unmanned aerial vehicles – known as drones – and the possible development of fully autonomous weapons systems – colloquially known as 'killer robots' – raise numerous critical questions for scholars and policymakers. In the case of cyber attacks, it will be necessary to determine exactly what constitutes an attack, if such an attack should fall under international humanitarian law (IHL) or the laws of armed conflict as an armed attack, and how to distinguish between civilian and military infrastructures. These interconnected issues have not yet created

* Correspondence to: Author's email: denisegarcia@neu.edu

a gaping legal hole or a new legal crisis, and therefore existing international law may suffice, however there are questions that need to be addressed. Cyberspace is digitised, which allows for greater anonymity, thus complicating the attribution of conduct. As the ability to enforce IHL depends on attribution of responsibility, if a perpetrator cannot be identified it is not clear how IHL can be applied. Such new technologies may raise the legal questions of what would be considered a legal attack, who would be considered the attacker, and what constitutes the battlefield. Fully lethal autonomous systems, when operational, will create many legal and ethical concerns that need to be addressed. It is not clear who can be held responsible for attacks, as one cannot hold a robot responsible. The programming of such robots raises concerns, as there needs to be agreement on what type of instructions they can receive. It is essential to determine whether international law and security governance are adequately keeping up with the development of new technologies.

My premises are twofold: one is that international security itself depends in part on the international regulation of armaments, as all states will have advantages arising from the value of having them either controlled or prohibited.[1] This central premise is embedded within the broader literature on institutionalism, security regimes, and non-proliferation and this analysis emphasises the importance of the dialogue between security studies and international law.[2] And second is that more cooperation and transparency in the domain of new lethal weapons technologies, in and out of the cyber world, mean more peace and security, while less coordination and no clear global governing rules mean a more insecure world.

I argue therefore that 'preventive security governance' could be a strategy to curtail uncertainty in the preservation of stability and international order. I define 'preventive security governance' as the codification of specific or new global norms, arising from existing international law that will clarify expectations and universally agreed behaviour on a given issue-area. Such issue-area is characterised by no rules or by the imprecision of extant rules.

This article applies this new concept to three interconnected areas of recent and future technological advance that may impinge upon the ability to protect civilian populations during peace and

[1] Others are in agreement with such views. Nico Krisch, 'The decay of consent: International law in an age of global public goods', *American Journal of International Law*, 108 (2014), pp. 1–40; see also Ian Hurd, 'The international rule of law and the domestic analogy', *Global Constitutionalism*, 4:3 (2015), pp. 365–95; Denise Garcia, 'Humanitarian security regimes', *International Affairs*, 91 (2015), pp. 55–75.

[2] For the related relevant literature on institutionalism, security regimes, and their ties with the scholarship on non-proliferation my arguments are embedded in, see Gene M. Lyons, 'A new collective security: The United Nations in theory and practice', *The Washington Quarterly*, 17:2 (1994); Edward Luck, 'Making peace', *Foreign Policy*, 89 (1992–3).

More specifically on non-proliferation, see Roger K. Smith, 'Explaining the non-proliferation regime: Anomalies for contemporary International Relations theory', *International Organization*, 41:2 (1987); Richard Betts, 'Systems for peace or causes of war? Collective security, arms control, and the new Europe', *International Security*, 17:1 (1992); George W. Downs and David M. Rocke, *Tacit Bargaining, Arms Races, and Arms Control* (Ann Arbor, MI: University of Michigan Press, 1990); Matthew Evangelista, 'Cooperation theory and disarmament negotiations in the 1950s', *World Politics*, XLII:4 (1990); Tanya Ogilvie-White, 'Is there a theory of nuclear proliferation? An analysis of the contemporary debate', *Nonproliferation Review*, 4:1 (1996), pp. 43–60; William C. Potter and Gaukhar Mukhatzhanova (eds), *Forecasting Nuclear Proliferation in the 21st Century: A Comparative Perspective* (Palo Alto, CA: Stanford University Press, 2010); Scott Sagan, 'Why do states build nuclear weapons? Three models in search of a bomb', *International Security*, 3:21 (1996/7), pp. 54–86; Rebecca Johnson, 'The NPT in 2004: Testing the limits', *Disarmament Diplomacy*, 76:March/April (2004).

war: drones; autonomous weapons systems; and the potential militarisation of cyberspace, or its use as a weapon, also considering the operation of drones and autonomous weapons systems in the cyber domain.[3] Drones depend on constant, real-time control by a human operator via communication systems involving cyberspace. This makes such systems vulnerable to cyber attacks, malware, hijacking, etc. It is uncertain whether future autonomous systems will no longer depend on real-time control by humans and will be able to operate independently from communication networks in cyberspace. Even though there are analytical differences and recognised distinctive legal ramifications among the three areas, I focus on the overarching characteristic that unites these areas: there is neither certainty nor proper specific governance, that is, no precise rules administering commonly agreed behaviour. Hence, this article pioneers a discussion of legal-political frameworks that can be utilised for the creation of preventive security governance in particular on cyber warfare and autonomous weapons systems due to the pronounced uncertainty arising from the lack of clarity on the application of existing international law. The robotics revolution is transforming military affairs as much as did the inventions of gunpowder and nuclear weapons: 'it is their nonhumanity that sums up their difference from all previous weapons'.[4]

Five fundamental concerns make the further use of armed drones, non-governance in the cyber domain, and the future deployment of autonomous weapons systems problematic. First is retrogression in the observance of accepted mores for global society and agreed-upon international law anchored on peace and security; second is the illegality of their extraterritorial use in the territories or cyberspaces of other countries at peace; third is the potential for them to become the prevailing technology of combat and fighting, and the main means of carrying out extra-judicial killings and anonymous attacks; fourth is the unpredictability of the technologies employed, which leads to inability to attribute culpability and accountability; and fifth is that ambiguity or lack of clarity on the existing global norms as applicable to these areas.

To develop these arguments, I start by introducing the applicable legal framework, and then situate my arguments within the debates on global governance of security, in particular 'new governance theory' that takes into account novel governance regulatory forms and actors who play a role in bringing them to fruition.[5] I then discuss the opinion of the Artificial Intelligence scientists' community. The literature I explore here has long recognised the value of 'epistemic communities' in guiding states in areas of technology and scientific complexity.[6] The scientists' views lend credence to my concept of preventive security governance as a mechanism to prevent future harm to civilian populations. Subsequently, the legal framework is discussed in three areas where the lack of clarity on the existing global legal architecture may imperil civilians in and out of conflict: *'preventing future harm to civilians'*, *'responsibility and accountability'*, *'what constitutes a legal and legitimate attack'*. To conclude, I summarise this first legal-political overview that conceptualises 'preventive security governance'.

[3] Denise Garcia, 'The case against killer robots – why the United States should ban them', *Foreign Affairs* (10 May 2014), available at: {www.foreignaffairs.com/articles/141407/denise-garcia/the-case-against-killer-robots} accessed 18 May 2014.

[4] Peter W. Singer, *Wired for War* (London and New York: Penguin Books, 2009), p. 14.

[5] John Gerard Ruggie, 'Global governance and "new governance theory": Lessons from business and human rights', *Global Governance*, 20:1 (2014), pp. 5–17.

[6] Peter Haas, 'Epistemic communities and international policy coordination', *International Organization*, 46:1 (1992), pp. 1–35.

Main arguments and the new governance theory

What makes drones, autonomous weapons systems, and the weaponisation of cyber space different from previously existing weapons, and what unites them?[7] The answer lies in the common underlying trends they set and their common features in transforming the nature of an attack. Here are three main arguments I develop: First, there are heated discussions of the legality and the legitimacy of the use of armed drones to conduct extrajudicial killings through extraterritorial targeting (targeted killings).[8] Even though there is nothing inherently illegal in the use of drones, and their remote operators may be fully able to comply with the rules of IHL, their current use may disrespect other branches of international law, such as Human Rights Law (HRL), and the rules on the legality of the use of force (*jus ad bellum*).[9]

I contend that the current use of armed drones in such ways signify a departure from significant protections entitled to individuals living in and out of conflict situations and therefore should be regulated by common norms of behaviour.[10] Even authors who believe there is nothing really more pernicious about the use of armed drones if compared to other weapons systems, would concur that commonly agreed rules should be clarified.[11] Current uses represent a trend towards increased resort to military force instead of diplomacy and negotiation. This trend warrants attention because their supposed expediency has accelerated the tendency to resort to them. Second, the delegation of tasks previously assumed by humans to machines makes offence and defence automated, and there is less use of kinetic force to achieve the same or bigger effects. In terms of the transformation of the nature of an attack, there is the difficulty of determining authorship and attribution (if more autonomy on the targeting and then on the decision to kill is delegated to machines) of acts that may be deemed illegal. This difficulty has the perverse effect of lowering the threshold for when and where these acts can occur and diminishing the sense of responsibility and morality. Third, the increasing dependence on technology may lead to more unanticipated susceptibility to technical failures. The Martens Clause, one of the first rules of IHL and binding by custom, prescribes the application of the principle of humanity during conflict – but 'taking humans out of the loop also risks taking humanity out of the loop'.[12] In sum, the connecting thread between drones, autonomous weapons systems, and cybernetics is the way each enables warlike actions to occur but without the traditional costs associated with them.

My arguments are situated within the 'new governance theory' that takes into account new governance regulatory forms, such as the preventive security governance framework I propose herein. This theory is defined as scholarly works that recognise the absence of global legal governing hierarchies and take into account the role played by non-state actors as well as international

[7] This question was posed by the International Committee of the Red Cross (ICRC), 'New technologies and warfare', *International Review of the Red Cross*, 94:886 (2012), p. 46.

[8] Jelena Pejic, 'Extraterritorial targeting by means of armed drones: Some legal implications', *International Review of the Red Cross*, 96:893 (2014), pp. 67–106.

[9] Stuart Casey-Maslen, 'Pandora's box? Drone strikes under *jus ad bellum*, *jus in bello*, and international human rights law', *International Review of the Red Cross*, 94:886 (2012), pp. 597–625; Janina Dill, *Legitimate Targets? Social Construction, International Law and US Bombing* (Cambridge: Cambridge University Press, 2014).

[10] Allen Buchanan and Robert O. Keohane, 'Toward a drone accountability regime', *Ethics and International Affairs*, 29:1 (2015), pp. 51–8.

[11] Michael J. Boyle, 'The legal and ethical implications of drone warfare', *The International Journal of Human Rights*, 19:2 (2015), pp. 105–26.

[12] Christof Heyns, UN Doc. A/HRC/23/47, 'Report of the special rapporteur on extrajudicial, summary or arbitrary executions', United Nations (9 April 2013), p. 17.

norms.[13] At the heart of the concept of 'preventive security governance' rests the idea of 'prevention', which as a framework for multilateral action is more theoretically developed in the environmental protection area,[14] and less so in the security governance area.[15] Here I explore frameworks for prevention utilising the new governance theory framework within the security governance realm. I add to the rich literature of security studies and push it in new directions. The new governance theory framework adds new actors who are essential in playing a role in finding solutions to the most significant global cooperation challenges. Other authors have explored the idea of 'prevention' in the disarmament and arms control area.[16] The dialogue between security studies and International Law that I explore in this article is needed to explain the role of new technologies and behaviours in international relations that may affect international security due to uncertainty. The role of epistemic communities that may work with states to navigate uncertainty is essential and I use it to further enhance the understanding of security governance in the literature.[17]

The literature on global governance has created valuable new roads for tackling problems in world politics; for some it has even rescued the field of International Relations studies from impracticality and invigorated it, making it more applicable to real-world problems.[18] The literature has made instrumental contributions in the areas of environment, trade and finance, and human rights; particularly prominent were the contributions on environmental governance, especially on climate (which is constituted of highly fragmented governance frameworks). Recognised and time-honoured examples of established global governance are in the areas of transportation, communications, and international trade that 'represented the low-hanging fruit of global cooperation. They were often technical in nature, offering practical solutions to problems that had to be resolved at a global level. Their acceptance did not require the surrender of sovereignty or the compromising of any nation's vital economic or security interests.'[19] The thematic arenas of economic, environmental, and human rights governance are dominant in the literature.[20]

[13] Ruggie, 'Global governance and "new governance theory"'.

[14] G. Marceau, 'The precautionary principle under WTO law', *Precaution from Rio to Johannesburg: Proceedings of Geneva Environmental Network Roundtable* (Geneva: International Environment House, 2002).

[15] D. Freestone and E. Hey (eds), *The Precautionary Principle and International Law: The Challenge of Implementation* (The Hague: Kluwer International, 1996).

[16] Jürgen Altmann, *Military Nanotechnology: Potential Applications and Preventive Arms Control* (New York: Routledge, 2006), chs 1–3.

[17] Elke Krahmann, 'Conceptualizing security governance', *Cooperation and Conflict*, 38:1 (2003), pp. 5–26; Frank Biermann, Philipp H. Pattberg, Harro van Asselt, and Fariborz Zelli, 'The fragmentation of global governance architectures: a framework for analysis, *Global Environmental Politics*, 9:4 (2009), pp. 14–40; Helen V. Milner, *Interests, Institutions, and Information: Domestic Politics and International Relations* (Princeton, NJ: Princeton University Press, 1997); Robert O. Keohane and Lisa L. Martin, 'The promise of institutionalist theory', *International Security*, 20:1 (1995); Barbara Koremenos, Charles Lipson, and Duncan Snidal (eds), *The Rational Design of International Institutions*, *International Organization*, 55:4 (Special Issue) (2001); Helga Haftendorn, Robert O. Keohane, and Celeste A. Wallander (eds), *Imperfect Unions: Security Institutions over Time and Space* (Oxford: Oxford University Press, 1999); Benjamin Miller, 'Explaining Great Power cooperation in conflict management', *World Politics*, 45:1 (1992); Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge: Cambridge University Press, 1990).

[18] Thomas G. Weiss and Rorden Wilkinson, 'Global governance to the rescue: Saving international relations?', *Global Governance*, 20:1 (2014), pp. 19–36.

[19] Nayan Chanda, 'Runaway globalization without governance', *Global Governance*, 14:2 (2008), pp. 119–25 (p. 123).

[20] H. Overbeek, K. Dingwerth, P. Pattberg, and D. Compagnon, 'Forum: Global Governance: Decline or maturation of an academic concept?, *International Studies Review*, 12:4 (2010), pp. 696–719.

The contributions to the area of security governance investigated, that is, how will states prepare to wage war and remain at peace in the future; and weapons and arms prescriptions and proscriptions, in particular of new technologies and future arms, are at the core of the global governance of security.[21] Present weapons procurement and future weapons development need to be the subject of more enquiry in the literature of global governance. High-profile attention to this domain has grown in prominence in the last 15 years, with new treaties on the prohibition of anti-personnel landmines and cluster munitions, the Arms Trade Treaty,[22] and the recent attempt to begin reframing the nuclear proliferation debate. Other areas of future weapons and related technologies, such as fully autonomous weapons systems and cyberspace, have also been receiving concerted international attention.[23] The attention to these security governance questions may reshape the understanding of international security and international law. Some of these matters have been examined as humanitarian questions – they have not been cast under a strictly 'security' light – but have been portrayed as 'humanitarian' imperatives which states have to embrace, or as moral and ethical concerns to be addressed to protect potential victims or save the world from larger humanitarian consequences.[24] These issues, essential for peace, war, and security in this century, deserve a rightful place in the literature of global governance especially as part of a dialogue between security and international law in which many different actors should be involved, included the scientists.

The opinion of the scientific community

The unique problems arising from lethal autonomous systems that may or may not be operated in the cyber world were highlighted in a historic letter by the world's foremost scientists on robotics and artificial intelligence in July 2015:[25]

> Autonomous weapons select and engage targets without human intervention. They might include, for example, armed quadcopters that can search for and eliminate people meeting certain predefined criteria, but do not include cruise missiles or remotely piloted drones for which humans make all targeting decisions. Artificial Intelligence (AI) technology has reached a point where the deployment of such systems is – practically if not legally – feasible within years, not decades, and the stakes are high: autonomous weapons have been described as the third revolution in warfare, after gunpowder and nuclear arms … In summary, we believe that AI has great potential to benefit humanity in many ways, and that the goal of the field should be to do so. Starting a military AI arms race is a bad idea, and should be prevented by a ban on offensive autonomous weapons beyond meaningful human control.

[21] Götz Neuneck, 'Ist die Bewaffnung des Weltraums unvermeidbar? Möglichkeiten und Aussichten für eine präventive Rüstungskontrolle im Weltraum', *Die Friedens-Warte*, 83:2–3 (2008), pp. 127–53.

[22] Denise Garcia, *Disarmament Diplomacy and Human Security – Regimes, Norms, and Moral Progress in International Relations* (London: Routledge, 2011).

[23] Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (New York: Oxford University Press, 2015); Brandon Valeriano and Ryan C. Maness, 'The dynamics of cyber conflict between rival antagonists, 2001–2011', *Journal of Peace Research*, 51:3 (2014), pp. 347–60; M. D. Cavelty, 'Cyber-security', in J. P. Burgess (ed.), *The Routledge Handbook of New Security Studies* (London: Routledge, 2010), pp. 154–62; P. W. Singer and A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2013).

[24] Denise Garcia, 'Humanitarian security regimes', *International Affairs*, 91:1 (2015), pp. 55–75.

[25] 'Autonomous Weapons: An Open Letter From AI & Robotics Researchers', Future of Life Institute, available at: {http://futureoflife.org/AI/open_letter_autonomous_weapons} accessed 3 August 2015.

A security governance option, as the AI scientists argue, would be a preventive prohibition under international law of the development and use of offensive lethal autonomous technologies. Part of this argument is also advanced by other epistemic communities (that is, groups that offer knowledge and technical advice for states), such as the Campaign to Stop Killer Robots and the International Committee for Robot Arms Control. These groups and epistemic communities advocate that the surest path for governance frameworks is a total preventive prohibition to delegate the decision to kill to machines (defensive and offensive lethal autonomous systems). Along the same lines, the promotion of commonly agreed norms on cybernetics in the United Nations to prevent the escalation of tensions in case of attacks, and to remedy problems arising from attacks in a cooperative way, will be essential. The scholarship on these areas is unanimous in arguing that autonomous lethal technologies are profoundly transformative of the face of warfare for three reasons: the threshold to initiate war will be lowered,[26] the hard ethical and moral decisions will be simplified for the sake of expedient use of technological shortcuts,[27] and especially humans will be out of the loop of the ultimate decision to kill, for the first time in history.[28] Thus even if such lethal technology is one day able to comply with IHL, it will disrespect international law, as I argue here.[29]

The making of global governance is in a predicament: on the one hand, new technologies are fast on the rise and have many positive civilian applications. On the other hand, how will humanity cope with the potential of new lethal technologies with implications for how warfare is waged and impending prospects for imperiling peace and security? Whether states adopt new controls or use existing international law is of relevance, in particular for new cyber technology as well as fully autonomous weapons systems. The existing rules on extrajudicial (targeted) killings are being contested because of the uncertain regulation of drones.[30] There is no clear governance in the areas of autonomous weapons systems and cyberspace. When fully operational, autonomous weapons systems are likely to make the existing prevailing practice of targeted killing more indeterminate.[31] The problems are the new and unanticipated costs that may arise in the future, leading to instability in the international system. Previous arms control and prohibition treaties targeted specific weapons categories, in most cases due to their harmful effect.[32] However, a preventive ban on autonomous weapons systems must focus on prohibiting the delegation of authority to kill to machines.[33]

The applicable legal framework

Five branches of international law can be examined to shed light on how preventive security governance could be built in the areas studied here: law of state responsibility, law on the use of force

[26] Sarah Kreps and Micah Zenko, 'The next drone wars', *Foreign Affairs*, 93:2 (2014), pp. 68–80.
[27] John Kaag, 'Military frameworks: Technological know-how and the legitimization of warfare', *Cambridge Review of International Affairs*, 22:4 (2009), pp. 585–607.
[28] Gwendelynn Bills, 'LAWS unto themselves: Controlling the development and use of lethal autonomous weapons systems', *George Washington Law Review*, 83:1 (2014), pp. 176–209.
[29] Louise Doswald-Beck, 'International humanitarian law and new technology', *American Society of International Law: Proceedings of the Annual Meeting* (Washington, DC: 2012), pp. 107–16.
[30] Nils Melzer, *Targeted Killing in International Law* (New York: Oxford University Press, 2008), chs 1 and 2.
[31] Heyns, UN Doc. A/HRC/23/47, 'Report of the special rapporteur'.
[32] Jürgen Altmann, Peter Asaro, Noel Sharkey, and Robert Sparrow, 'Armed military robots: Editorial', *Ethics of Information Technology*, 15:2 (2013), pp. 73–6.
[33] Peter Asaro, 'On banning autonomous weapon systems: Human rights, automation, and the dehumanization of lethal decision-making', *International Review of the Red Cross*, 94:886 (2012), p. 696.

(*jus ad bellum*), IHL (*jus in bello* or the laws of armed conflict), HRL, and what I term the 'law of the commons'. Authors have devoted attention to IHL due to its application in times of conflict. Nonetheless, future technologies will be used outside areas of conflict, for normal law enforcement, and especially within cyberspace. Robots are already utilised in law enforcement in several countries. Thus it is important to examine the range of existing law that could be used for states to create a basis for preventive security governance. These branches are analysed to assess whether they form the basis for the creation of security governance frameworks in areas that may jeopardise peace and stability and imperil civilian populations. Among these international law branches, IHL has played a continuous role in either prohibiting or restricting new and existing weapons throughout history, and was created, modified, and refined on several occasions – 1864, 1899, 1907, 1929, 1949, and 1977 – to enhance the protection of civilian populations, setting limits for conduct during war and limiting armaments, with clarification and adaptations to reflect evolving customary law. Do IHL and other branches of international law now have to be amended or modified, or do their existing fundamental principles that pose restrictions on arms remain valid and resilient? The guardian and custodian of IHL, the International Committee of the Red Cross (ICRC) takes the position that IHL applies to new weaponry and technological developments. The problem is one of terminological clarity in the legal application of extant rules and norms to new weapons, in particular in limiting and impeding unwanted humanitarian consequences.

It is critical to determine how existing branches of international law apply to protect civilians from harm,[34] and whether what currently exists is sufficient to address the challenges posed by the development of new weapons and technologies.[35] Some authors affirm that existing frameworks are, in principle, sufficient.[36] In addition, the fact that a particular means or method of warfare is not specifically regulated does not mean that it can be used without restriction.[37] This does not, however, mean that laws cannot be strengthened or that new laws do not need to be created to address future arms and technologies.[38] How to clarify existing governance frameworks and what they should include if new architectures are created pose difficult questions.

Preventing future harm to civilians

IHL does not prohibit technological developments, but these must be measured and assessed against existing legal norms. How can one prevent large-scale calamities caused by the use of future weapons and technologies? History works against preventive norm making. States usually react, as technological developments usually outpace political agreements to tackle future potential problems.

[34] Kenneth Anderson, Daniel Reisner, and Matthew Waxman, 'Adapting the law of armed conflict to autonomous weapon systems', *International Law Studies*, 90 (2014), pp. 386–411, available at: {https://www.usnwc.edu/getattachment/a2ce46e7-1c81-4956-a2f3-c8190837afa4/Adapting-the-Law-of-Armed-Conflict-to-Autonomous-We.aspx} accessed 15 September 2014.

[35] ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts', paper presented at 31st International Conference of the Red Cross and Red Crescent, Geneva, 28 November–1 December 2011.

[36] Matthew Waxman and Kenneth Anderson, 'Law and ethics for autonomous weapon systems: Why a ban won't work and how the laws of war can', Council on Foreign Relations (13 April 2013), available at: {www.cfr.org/drones/law-ethics-autonomous-weapon-systems-why-ban-wont-work-laws-war-can/p30445} accessed 21 November 2013.

[37] Sarah Kreps with John Kaag, 'The use of unmanned aerial vehicles in asymmetric conflict: Legal and moral implications', *Polity*, 44:2 (2012), pp. 260–85.

[38] Marco Sassoli, 'Autonomous weapons and international humanitarian law: Advantages, open technical questions and legal issues to be clarified', *International Law Studies*, 90 (2014), pp. 308–40.

This is because most international treaties and other global policy actions at the international level are driven by evidence, data, and campaigns.[39] It is challenging to create a campaign without evidence, without problems having already materialised. Thus the debate has to be about the preventive humanitarian imperative and the human cost that may ensue. Shifting the burden of military utility is key.[40] Historically, two weapons systems have been banned preemptively (expanding bullets in 1899 and blinding lasers in 1998) because they were designed to produce 'superfluous injury'. Usually, states are against pre-emptive weapons bans *a priori*. It is very hard to create global momentum without evidence of existing problems.

Along the same lines, the emergence of the possibility of wars in cyberspace means we have now opened up another area beyond the oceans, land, and outer space where hostilities can occur. Reconciling the extant legal framework that now governs armed conflict with this reality where interconnectedness without borders is the new norm is rather challenging.[41] In the IHL realm, Additional Protocol I to the Geneva Conventions takes the necessary precautions to protect the civilian population, individual civilians, and civilian objects under their control against dangers resulting from military operations. States therefore are also under a customary obligation to take precautions against the effects of armed attacks on civilian populations.[42]

In terms of a general legal obligation, IHL constitutes a foundational basis in situations of conflict, but beyond conflict, and in all other conditions, it has to be considered with HRL. If this law is breached, the determination of legality through the prism of the other branches is even more vulnerable to unlawfulness. Thus the starting point is the consideration that the use of force is permissible in two classic instances: one is in self-defence, and the other is with the authorisation of the UN Security Council. In general, self-defence cannot be retaliatory or punitive and can only repel an actual attack – for instance, right after 9/11 with the Security Council's authorisation of the lawful use of force in Afghanistan. The use of drones by one state to target individuals located in another state is lawful if it complies with the law on the use of force. Many would support the use of force in the territory of other countries as 'anticipatory self-defence', but this view does not find legal ground in international law.

The current use of armed drones, their continuing application in the territory of countries where no war is declared, and the probable employment of autonomous weapons systems in the future to carry out policies of extrajudicial killings are a 'fundamental regression in the evolution of both international law and United States domestic law'[43] and a retreat to what Thomas Jefferson in 1789 argued was a mediaeval practice of assassination from the dark ages.[44] Even though, the current

[39] Charli Carpenter, *'Lost' Causes: Agenda Vetting in Global Issue Networks and the Shaping of Human Security* (New York: Cornell University Press, 2014).

[40] John Borrie, 'Humanitarian reframing of nuclear weapons and the logic of a ban', *International Affairs*, 90:3 (2014), pp. 625–46.

[41] Robin Geiß and Henning Lahmann, 'Cyber warfare: Applying the principle of distinction in an interconnected space', *Israel Law Review*, 45:3 (2012), pp. 381–99.

[42] Cordula Dröge, 'No legal vacuum in cyberspace', ICRC online interview (16 August 2011), available at: {https://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm} accessed 22 September 2014.

[43] Philip Alston, 'The CIA and targeted killings beyond borders', Public Law and Legal Theory Working Paper No. 303, New York University (16 September 2011), p. 4.

[44] Letter from Thomas Jefferson to James Madison, 28 August 1789, in Julian P. Boyd (ed.), *The Papers of Thomas Jefferson*, 15:367 (1958).

American policy on the use of armed drones is done within a framework of self-defence under international law that is being extended since the authorisation of the use of force in 2001.

Nils Melzer's[45] definition of extrajudicial targeted killings is the use of lethal force with some sort of weapon that involves intent, premeditation, and deliberation to kill as part of a specific policy, directed at selected individuals not under the physical custody of the executor, who has to be a subject attributable to international law. The larger question within the debate on the lawfulness of targeted killings resides in what Peter Singer calls 'the conflation of the tactics and the technology'.[46] Are people concerned about the technology (armed drones) that is being used in places with which the US is not at war, or about the tactics?[47] The latter seems to be the answer, but the perception of the results is aggravated by the fact that the technology (armed drones) promotes a 'neutralizing' distance between the executor and the victim. In the case of autonomous weapons systems, there will be no conflation because the robot will decide on the tactics as well. Will this be more acceptable, or make matters worse? There seems to be a wide recognition in the legal scholarship that targeted killings are usually illegal. Even in the extremely narrow circumstances where they are legal (if able to be justified), they are perceived as illegitimate with no public accountability.[48] When is it ever legitimate under HRL to deprive a human being of life without the presumption of innocence and right to trial? The answer is in situations of conflict: during hostilities it is lawful to target a combatant, according to Article 3 common to the Geneva Conventions, with the arising obligation of distinction between combatants and non-combatants. Otherwise, under HRL, depriving a human being of life is rarely legal.

Can we assume that this existing legal framework imposes significant constraints on hostile cyber activities, for instance? First, in terms of UN Charter Article 2.4 that prohibits the use of force, do cyber attacks or the use of drones constitute a breach of the international norm against the use of force?[49] Second, in terms of Article 51 that establishes the main norm allowing self-defence, could a cyber attack give rise to a right to use military force in response? Third, do you envisage states renouncing the use of force in cyberspace or extending UN Charter Article 2.4 to the cyber world?[50]

Another way to ascertain precaution is through the primacy of HRL, which rests on the protection of the right to life. Indiscriminate and arbitrary (targeted) killings are unlawful through both treaty and customary law, and this represents a consolidated international norm. Central to the determination of an action's legality is the International Covenant on Civil and Political Rights (one of the main international treaties in the HRL legal regime): Article 6 enshrines the right to life,[51] and Article 4.2 assures its non-derogability as an essential component of HRL. The observance of the right to life is considered to be a peremptory or non-derogable rule of international law. According to the International Court of Justice (ICJ), even if a means of war does not violate international law,

[45] Nils Melzer, *Targeted Killing in International Law* (London and New York: Oxford University Press, 2010).
[46] Singer, *Wired for War*.
[47] David Kretzmer, 'Targeted killing of suspected terrorists: Extra-judicial executions or legitimate means of defence?', *European Journal of International Law*, 16:2 (2005), p. 171.
[48] Philip Alston, UN Doc. A/HRC/14/24/Add.6, 'Report of the special rapporteur on extrajudicial, summary or arbitrary executions. Addendum: Study on targeted killings' (28 May 2010).
[49] Sarah Knuckey, *Drones and Targeted Killings: Ethics, Law, Politics* (New York, IDebate Press, 2014).
[50] Matthew Waxman, 'Cyber-attacks and the use of force: Back to the future of Article 2(4)', *Yale Journal of International Law*, 36 (2011).
[51] UN General Assembly, 'International Covenant on Civil and Political Rights', United Nations Treaty Series, Vol. 999, Article 6 (16 December 1966).

it may still breach the dictates of public conscience through the Martens Clause. This clause first appeared in the Hague Conventions, and then was reiterated in multiple instruments of IHL. The Martens Clause prescribes that until a fuller international guideline exists, populations at war remain under the protection of the principles of international law and those of humanity, according to practice accepted by civilised nations and public conscience. Thus by custom states are prescribed to evaluate the moral and ethical repercussions of new technologies. It is widely recognised that HRL is also applicable in times of conflict, and in cases of intentional or arbitrary deprivation of life.[52]

The question before the international community here is how existing international law protects civilians: who is to be held accountable and deemed responsible for wrongdoings committed during both conflict and peace situations (that is, law enforcement)? Essentially, under what conditions will protection and accountability be assured when future arms and technologies are fully operational?

Responsibility and accountability

The law of state responsibility provides a general codified framework containing the essential rules of international law *vis-à-vis* the responsibility of states regarding their wrongful acts.[53] They represent in many ways a fundamental framework for limiting state freedom on conduct in international relations, and could be a theoretical legal basis for holding states accountable for conduct at the international level,[54] especially in case of violation of peremptory norms in the creation of new frameworks for security governance. Peremptory norms (*ius cogens*) are 'accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character'.[55] One example illustrating this is the norm against aggression – pertinent for attacks in cyberspace and possible uses of automated warfare that will likely reduce the thresholds for the use of force.

An internationally wrongful act may elicit state responsibility when conduct consisting of an action or omission is attributable to the state and constitutes a breach of an international obligation of the state to previously assumed responsibilities. The law of state responsibility is concerned with the determination of whether there is a wrongful act for which the state is to be held responsible, what the legal consequences are, and what reparations should be taken. The law of state responsibility represents a valuable legal framework under *ius cogens*, such as the norm protecting the right to life and the norm against the use of force, which may be commonly violated. The road to full automation of warfare or the use of cyberspace for attacks will likely create additional violations because attribution and responsibility will be hard to determine. In the case of autonomous weapons systems, the question of legal responsibility could be overriding: if responsibility cannot be attributed, then a responsibility vacuum would emerge.[56] It will be difficult to ascertain whom to hold responsible for a

[52] International Court of Justice, 'Legality of the threat or use of nuclear weapons: Advisory opinion', *ICJ Reports* (8 July 1996), p. 226, para. 25.

[53] James Crawford, *The International Law Commission's Articles on State Responsibility* (Cambridge: Cambridge University Press, 2002).

[54] International Law Commission, 'Responsibility of states for internationally wrongful acts', *Yearbook of the International Law Commission*, II:2 (2001), p. 31, available at: {http://www.un.org/documents/ga/docs/56/a5610.pdf} accessed 14 August 2014.

[55] United Nations, 'Vienna Convention on the Law of Treaties', United Nations Treaty Series, Vol. 1155, Article 35 (23 May 1969), p. 331.

[56] Heyns, UN Doc. A/HRC/23/47, 'Report of the special rapporteur'.

killer robot's actions, as no human took the final decision, and the same can be said of cyber warfare.[57] How to take precautions and assess what could be proportional attacks are essential for the determination of state responsibility.

IHL has chiefly established rules governing the determination of the proportionality of the use of force during hostilities in order to avoid indiscriminate attacks against vulnerable populations.[58] It represents an essential branch of law because its far-reaching obligations are commanding, due not only to its constituting the Geneva Conventions of 1949 and their additional protocols, but also to its customary character. The evolution of restrictions on methods of warfare has occurred in two tracks in the last 150 years: one, general principles and rules that apply to all means of warfare; and two, specific treaties that have either prohibited or regulated certain types of weapons systems.[59] The ICRC posits that IHL is applicable to all new weaponry and new technology; this derives in part from Article 36 of Addition Protocol I that mandates states to conduct reviews of new weapons. According to this view, extant IHL therefore applies to new technology because it is not the nature of the means and methods that triggers IHL, but the context and the humanitarian consequences.[60] However, this framework is applicable only in situations of armed conflict, and leaves open the question of whether future arms will be used and cyber attacks will occur during peace.[61] The possibility that the weapons may be used in circumstances outside of armed conflict requires comprehensive attention, because actually most future arms and technologies will be used in situations of peace, most prominently in law enforcement circumstances.[62] Article 36 is also concerned with future weapons.[63] There are problems, though: for instance, the secrecy surrounding the drones program *vis-à-vis* reviews, targets, and objectives does not foretell transparency and raises doubts that states will abide by IHL when full automation is in place. Even though weapons reviews are a requirement under international law, and also considered a customary requirement among nations, only a handful of states carry out weapons reviews regularly. In sum, the Article 36 obligation is not sufficient as a tool for preventive security governance in creating security frameworks for future arms and technologies. The central question of proportionality, which includes the decision to apply lethal force, is probably unworkable in lethal autonomous weapons systems and has to be weighed in dynamic environments that require highly qualitative and subjective knowledge.[64]

[57] Heather Roff, 'Gendering a warbot: Gender and lethal autonomous weapons', *International Feminist Journal of Politics* (2015).

[58] Heather Roff, 'Lethal autonomous weapons and proportionality', *Case Western Reserve: Journal of International Law*, 47 (2015), pp. 37–52.

[59] Jakob Kellenberger, 'International Humanitarian Law and New Weapon Technologies', Keynote Address, International Humanitarian Law and New Weapon Technologies, 34th Round Table on Current Issues of International Humanitarian Law, San Remo, 8–10 September 2011.

[60] Nils Melzer, 'Cyber Operations in *jus in bello*', *Confronting Cyberconflict*, United Nations Institute for Disarmament Research, UNIDIR, Geneva, Switzerland (2012).

[61] Suresh Guptara, UNIDIR Cyber Stability Seminar 2015: Regime Coherence, UNIDIR, Geneva (2015), available at: {http://www.unidir.org/files/publications/pdfs/cyber-stability-seminar-2015-en-636.pdf} accessed 11 January 2015.

[62] Christof Heyns, UN Doc. A/HRC/26/36, 'Report of the special rapporteur on extrajudicial, summary or arbitrary executions', UN Human Rights Council (1 April 2014).

[63] J. M. Henckaerts and L. Doswald-Beck (eds), *Customary International Humanitarian Law* (Cambridge: Cambridge University Press, 2005), p. 427.

[64] Noel Sharkey, 'Automating Warfare: Lessons Learned From the Drones', University of Sheffield (2012), available at: {www.alfredoroma.it/wp-content/uploads/2012/05/Automated-warfare-Noel-Sharkey.pdf} accessed 15 August 2014.

Underlying the key principles of IHL (those with treaty and customary force under international law) is the distinction between civilians and combatants, and the ensuing prohibition of indiscriminate attacks.[65] Following from this premise, the key principles are precaution, proportionality, and an appropriate choice of weapon that is not unlimited and articulates the proscription on weapons that are by nature indiscriminate and cause unnecessary suffering or superfluous injury.[66] Several conventions regulate or prohibit the use of specific weapons, including biological and chemical weapons, anti-personnel mines, cluster munitions, and blinding laser weapons. Furthermore, there is a balance between military necessity and humanitarian needs, safeguarded by a general principle of proportionality in which no force should be used beyond what is needed to achieve a desired military result.[67] In sum, there are two overarching customary principles on the use of weapons that have been codified in Article 35 of Additional Protocol I: one is that the use of means and methods of warfare whose nature causes superfluous injury or unnecessary suffering is prohibited. According to state practice, this rule is, as a norm of customary international law, applicable in both international and domestic armed conflicts. This widely agreed-upon prohibition implies the results of use of particular weapons, and is valid for weapons that have no military purpose or a purpose that outweighs their military utility and advantage.[68] The other principle consists of a proscription of weapons that are indiscriminate by nature and therefore cannot distinguish between civilians and combatants or be limited solely to a military objective. This is also viewed as a rule of customary international law.

A major challenge is the application of the principle of distinction when civilian and military cyber infrastructures are closely interconnected.[69] Anonymity of attacks is also problematic. IHL is a law of attribution.[70]

> The application of the accepted legal definition of military objectives in the interconnected cyber domain will render basically every cyber installation a legitimate military objective. In cyberspace, every component of the cyber infrastructure is a dual-use object. After all, by and large the military uses the very same cyber infrastructure that is used for civilian purposes.[71]

Many observers affirm that IHL is the surest branch of international law applicable to cyber warfare, because its principles represent a *ius cogens* foundation that is non-derogable.[72] The use of armed force, as per the ICRC definitions of armed conflict, does not necessarily trigger the application of IHL, but if cyber operations are intended to harm the adversary and cause injury, death, or destruction as well as to impair military capacity, they are subject to the full protection of IHL because they are considered as hostilities.[73] In other words, IHL is an effects-based branch of international law, and if the attacks constitute hostilities in the context of an armed conflict, then IHL applies.[74] In general, it is not what the weapon is or its nature but the effects, especially

[65] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*.
[66] These principles are codified in Additional Protocol I, Part III, § I.
[67] This principle is codified in Additional Protocol I, Articles 51, 57, and 58.
[68] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, chs 1–8.
[69] Yuval Shany and Nigel Rodley, 'Introduction', *Israel Law Review*, 45:3 (2012), pp. 379–80.
[70] Dröge, 'No legal vacuum in cyberspace'.
[71] Robin Geiß and Henning Lahmann, 'Cyber warfare: Applying the principle of distinction in an international space', *Israel Law Review*, 45:3 (2012), pp. 381–99.
[72] US Department of Defense, *An Assessment of International Legal Issues in Information Operations* (2nd edn, Washington, DC: US Department of Defense Office of the General Counsel, 1999).
[73] Nils Melzer, 'Cyber Operations in *jus in bello*', p. 25.
[74] Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), p. 13.

humanitarian, that elicit protection under IHL.[75] In addition, it is prohibited to employ arms to cause unnecessary suffering; this provision and the proscription of infliction of superfluous injury are together known as the Martens Clause.[76] Affirming and strengthening this, it is worth noting that most of the substantive provisions of the Hague Conventions are considered customary international law and therefore are binding on states which are not formally parties to them.[77] The ICJ reiterated the validity of the Martens Clause in its advisory opinion on the legality of the threat or use of nuclear weapons, affirming it has customary force; of special relevance is the affirmation that the clause constitutes a preliminary basis for the establishment of security governance frameworks.[78] Nevertheless, there are many uncertain areas in the determination of international responsibility and the nature of attacks that are likely to be aggravated with the fast evolution of military technology.

A legal and legitimate attack

When discussing new technologies, there are concerns *vis-à-vis* the determination of what may constitute an attack: the first is uncertainty, and the resulting potential inability to safeguard security of civilians even if all new technologies comply with the existing law. Second is the apparent underlying trend in all new weapons technologies that they will further remove the executor from the results of acts beyond any state's borders. This trend has consequences for respect for the rule of proportionality (avoidance of collateral damage and civilian loss) in the way the law understands and interprets it right now.[79] Third is transparency of use and uncertainty over the effects of use of existing and future weapons on civilian populations. Transparency in the assessment of use is fundamental for determining the application of the law. Fourth, responsibility and accountability *vis-à-vis* use and deployment remain unsure; especially if IHL is to be applicable, attribution must be identifiable.[80] In sum, IHL calls for 'attributability' of attacks.[81] The use of armed drone technology demonstrates that the initiator of the use of force can be far removed from where it is deployed. Autonomous weapons systems would increase this distance and detachment, which could make the determination of what constitutes an attack and who initiated it even harder. If this uncertainty is compounded by attacks in the cyber domain, the attribution of culpability will be even more difficult to ascertain.

The law of the commons may offer a basic minimal legal framework for the creation of security governance frameworks against cyber attacks that occur or originate in areas viewed as the common heritage of humanity.[82] The traditional areas of the international commons include the atmosphere,

[75] Nils Melzer, 'Towards a Code of Conduct for Cyber Space', paper presented at International Humanitarian Law and New Weapon Technologies, 34th Round Table on Current Issues of International Humanitarian Law, San Remo, 8–10 September 2011.

[76] Theodor Meron, 'The Martens Clause, principles of humanity, and dictates of public conscience', *American Journal of International Law*, 94:1 (2000), pp. 78–89.

[77] D. Schindler and J. Toman, *The Laws of Armed Conflicts* (Dordrecht: Martinus Nijhoff Publishers, 1988).

[78] International Court of Justice (1996), p. 226, paras 78 and 87.

[79] ICRC, Report of the ICRC Expert Meeting on 'Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects', 26–8 March 2014, Geneva, available at: {https://www.icrc.org/eng/assets/files/2014/expert-meeting-autonomous-weapons-icrc-report-2014-05-09.pdf} accessed 11 November 2015.

[80] Daniel N. Hammond, 'Autonomous weapons and the problem of state accountability', *Chicago Journal of International Law*, 15:2 (2015), pp. 652–88.

[81] Peter Spoerri, 'Conclusions', paper presented at International Humanitarian Law and New Weapon Technologies, 34th Round Table on Current Issues of International Humanitarian Law, San Remo, 8–10 September 2011.

[82] Scott J. Shackelford, 'The tragedy of the common heritage of mankind', *Stanford Environmental Law Journal*, 28 (2009a), p. 109.

the high seas, Antarctica, and outer space. This branch of international law has developed commonly agreed rules which expect cooperation and attainment of the aspirations of collective utilisation of the commons. For instance, the main treaty in space law, the 1967 Outer Space Treaty, instructs states to exploit outer space, including the moon and other celestial bodies, in a manner that benefits the interests of all countries, irrespective of their degree of economic or scientific development. By the same token, outer space, including the moon and other celestial bodies, shall be the province of all mankind and not subject to national appropriation by claim of sovereignty, nor the installation of weapons.[83]

In the making of novel security governance frameworks, cyberspace could be considered as part of what are known as common heritage of humanity areas, or 'international commons'. There are five noteworthy characteristics of the common heritage areas that can be potentially used for cyberspace. First, these areas cannot be nationalised, that is, no state can claim jurisdiction over them. Second, all nations must cooperatively manage the commons. Third, all must share the benefits deriving from the commons (which in many senses is already happening). Fourth, and very importantly, no militarisation of these areas is allowed. Fifth, intergenerational equity should be preserved, in the sense that future generations should benefit as much as present generations do.[84] 'In other words, cyberspace has eroded the connection between territory and sovereignty.'[85] Concurrently, the implications of disruption of satellite reception and transmission require pressing attention within the framework of preventive security governance explored here.[86]

A prominent idea for an initial framework for security governance is to renounce the use of force in cyberspace – extending UN Charter Article 2.4 to the cyber world.[87] A new international treaty with an inbuilt standing emergency response body would be the most comprehensive solution. Existing international law would be applicable to cyber attacks and threats, but in a haphazard and unsystematic way.[88] Many authors think a new treaty is unlikely because of deep security distrust among the 'cyber powers', even though there seems to be international consensus around the urgent need for standards of behaviour in cyberspace.[89] Parts of the issue have been the subject of conversation by groups of states at the UN, but the prospects for development of law in this area are dim.[90] State practice will probably develop heterogeneously and at an uneven pace. Most dangerously, it is probably the case that state practice will advance only as a reaction to major events, after the harmful effects have been felt.[91] A few observers consider that customary law constitutes a good basis to create commonly agreed rules to regulate the cyber world. This is premised upon two notions. One is the indiscriminate nature of the attacks for the target

[83] United Nations, UN Doc. A/RES/2222 (XXI), 'Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies' (Outer Space Treaty).
[84] Scott J. Shackelford, 'From nuclear war to net war: Analogizing cyber attacks in international law', *Berkeley Journal of International Law*, 25:3 (2009b), pp. 209–213 (p. 214).
[85] Ibid., p. 214.
[86] Deborah Housen-Couriel, 'Disruption of satellite transmissions *ad bellum* and *in bello*: Launching a new paradigm of convergence', *Israel Law Review*, 45:3 (2012), pp. 431–58.
[87] Ibid., p. 29.
[88] Shackelford, 'From nuclear war to net war', p. 214.
[89] Melzer, 'Towards a code of conduct for cyber space'.
[90] Matthew Waxman, 'Cyber warfare: Is There a Need for New Law?', paper presented at International Humanitarian Law and New Weapon Technologies, 34th Round Table on Current Issues of International Humanitarian Law, San Remo, 8–10 September 2011.
[91] Melzer, 'Cyber operations in *jus in bello*', pp. 3–14.

population: innocent people will suffer as a consequence.[92] The second is the fundamental interest states have in a stable international system that is founded on the free and steady flow of information, and therefore must be protected.[93] Anthony D'Amato draws an analogy to an old branch of international law, the law of diplomacy that first only had customary rules that then were enshrined and codified into treaty law as a governance framework accepted by all nations. I would say piracy was considered illegal first by customary law and then by treaty law in the same way. This precedent may constitute a creative framework for the drafting of security governance on lethal autonomy technology and in cyber diplomacy.

There are three main challenges in reconciling the existing governing framework of international law and the relatively new domain of cyber conflict in the determination of attacks. First is the difficulty of attribution of conduct because of the often-found anonymity shrouding cyber attacks; this will determine whether IHL may or may not be applicable. Second, can an 'attack' purely conducted by cyber means constitute an 'armed attack' under the Geneva Conventions? The ICRC says determining this in a definite manner will need future state practice. Third, the definition of 'attack' is central for triggering the application of the various rules of IHL. According to Article 49.1 of Additional Protocol I, 'attacks' means acts of violence against an adversary, whether in offence or defence. The ICRC interprets 'acts of violence' as meaning physical force, so extending the application of this to the cyber world would have to entail physical harm to people and structures.

Views are inconclusive about the application of IHL to cyber warfare and to future arms and new technologies, to a great extent. Existing international law will be applicable when more state practice occurs. IHL, for instance, is triggered solely in situations of armed conflict. All the three issue areas examined here maybe deployed in any other situations.[94] This leaves us in uncertainty: 'current norms do not sufficiently regulate some of the challenges posed [by new technologies and weapons] and might need to be elaborated'.[95]

In sum, the development of new technologies is not occurring in a legal vacuum, but the pressing issue is that there are uncertainties in the application of existing law to new weapons, and this is problematic for two reasons. First, there is the question of clarity of the existing rules *vis-à-vis* future weapons and new characteristics.[96] Second, uncertainty also surrounds the prevention of possible harmful humanitarian consequences of new weapons and whether the law will suffice.[97] Current international law is not enough for autonomous systems or attacks and uses in cyberspace. The surest path for creating security governance frameworks for future lethal autonomous technologies is the formation of an international treaty that will preventively prohibit them; in addition, a clear set of rules should be drafted in the United Nations on the prevention of cyber warfare and cyber attacks. Preventive security governance would then reduce the current peril of the uncertainty of existing legal frameworks.

[92] Anthony D'Amato, 'International law, cybernetics, and cyberspace', *Computer Network Attack and International Law*, Naval War College International Law Studies Blue Book, 76 (1999), pp. 59–71.
[93] Stephen J. Lukasik, 'Protecting the global information commons', *Telecommunications Policy*, 24:6 (2000), pp. 519–25.
[94] Dröge, 'No legal vacuum in cyberspace'.
[95] ICRC, 'International Humanitarian Law', p. 41.
[96] Shackelford, 'From nuclear war to net war'.
[97] ICRC, 'International Humanitarian Law'.

Conclusions

This article attempted to contribute to the global governance literature, furthering a dialogue between law and security, by focusing on the role of future arms and technologies in the potential deterioration of international security. I argued that the creation of security governance frameworks on future arms and technologies, commonly agreed by countries in the United Nations, is pressing. Theoretically, the arguments developed reasoned with the 'new governance theory' that finds the role of non-state groups (here epistemic communities are prominent) and the centrality of new norms are essential to fill in action and policy gaps in problems of cooperation. My premise is that no clarity on the global legal-political architecture in the domain of new and future lethal weapons technologies is precarious for order and security. And this assumption rests on the belief that international security itself depends in part on the international regulation of armaments, therefore it is in the interests of states to create preventive security governance frameworks to have them either controlled or prohibited. In the cases argued, in particular new lethal technologies in the realm of artificial intelligence, I contend that even if they may one day be able to abide by IHL, they will disrespect other rules of international law, making their development less than desirable for the protection of civilians and the future of international stability.[98]

I am in company with authors pointing to the fact that robots cannot discriminate between civilians and combatants,[99] and suggest that autonomous weapons systems would not be able to apply the rules of IHL because of the defectiveness of certain technologies – sensors, for instance – or when several different algorithms originating from different countries confront each other during the fog of war and in cyberspace. This would lead to unpredictable situations. The difficulties of identifying non-combatants could be glaring, and even more conspicuous would be the intricacies of translating these into computer software. During hostilities, compassion and intuition are often key human traits. Robots may be more pragmatic in a number of situations and be able perhaps to act with no passion, which can be useful. However, it is the ability to interpret and make compassionate judgements that robots may lack. All these uncertainties could result in a gap in assessing accountability: who could be held accountable, the hardware manufacturer, the software programmers, the military commanders, or the subordinates carrying out the fire-and-forget commands? More importantly, why would military commanders want to be removed from the most crucial decisions regarding life and death during war? What would this say about the future for humanity?

My concern is with the resulting vacuum of moral responsibility that could ultimately hinder international law and its goal of keeping a modicum of global security governance. The creation of multilaterally agreed norms on cybernetics will be essential and the meetings that are taking place in the United Nations are instrumental.[100] Along the same lines, the lack of accountability is exacerbated by the absence of transparency in development and potential use of such new technologies, as very few countries comply with the obligation to carry out weapons reviews to assess their legality. Moreover, the vagueness and lack of precision in applying the existing international law are contributing factors in undermining the rule of law upon which international security depends.

[98] Mary Ellen O'Connell, *21st Century Arms Control Challenges: Drones, Cyber Weapons, Killer Robots, and WMDs*, 13 Wash. U. Global Stud. L. Rev. 515 (2014).

[99] Noel Sharkey, 'Grounds for discrimination: Autonomous robot weapons', *RUSI Defence Systems* (October 2008), available at: {http://rusi.org/downloads/assets/23sharkey.pdf} accessed 21 November 2013.

[100] Garcia, *Disarmament Diplomacy and Human Security*, ch. 1.

Taken together, lethal robotic technologies raise practical questions. Is technology able to meet the requirements of international law, along with the intertwined civilian-military dual-use nature of the technology? Who is to be held accountable, especially if the primary actor is not a moral agent for command and responsibility? What does it do to our identity as humankind, and why forgo humans' unique capacity to engage in moral reasoning during war? In the end, questions of state responsibility abound. International law in this case provides some constraints, but it does not provide clear answers for future arms and technologies. As the world's foremost scientists on artificial intelligence recently warned the international community, for the future of humanity a preventive prohibition of offensive lethal autonomous technologies that are out of human meaningful control should be put in place now. The delay in the creation of preventive security governance frameworks happens at the peril of international security and the protection of civilians in and out of conflict.

Acknowledgements

Initial versions of this article were presented at the annual Cornell/International School on Disarmament and Research on Conflicts meeting in Italy in January 2013, and at the Cornell University Law School International Law & International Relations Colloquium in October 2013, and to my Conflict and International Negotiations classes at Northeastern University in 2014. I am thankful to the participants for constructive feedback. I am grateful to Maisam Alahmed, Matthew Cohen, Cherry Ekins, Timothy Edmunds, Matthew Evangelista, Sinja Graf, Judith Reppy, Sarah Kreps, Odette Lienau, the editors and four anonymous reviewers for insightful and helpful comments.

Biographical information

Denise Garcia is the Sadeleer Research Faculty and Associate Professor in the Department of Political Science and the International Affairs programme at Northeastern University in Boston. She teaches International Law and Global Governance in Boston and at the United Nations in Geneva. She is the author of *Small Arms and Security – New Emerging International Norms*, and *Disarmament Diplomacy and Human Security – Norms, Regimes, and Moral Progress in International Relations*. Garcia is the Vice-Chair of the International Committee for Robot Arms Control and a member of the Academic Council of the United Nations. Her articles have appeared in *Foreign Affairs, International Affairs, Ethics & International Affairs, Third World Quarterly, Global Policy Journal, International Relations*, among others.