Finding a Path Through The Autonomous Weapon Systems Stalemate

By

Tyne Schofield

A dissertation submitted to the Victoria University of Wellington

in partial fulfilment of the requirements for the

degree of Master of Laws

Victoria University of Wellington

2022

Contents:

Abstract:

Despite many years of debate, international agreement on what should be done to mitigate the risks of autonomous weapon systems is far from agreed. Critics suggest we desperately need a prohibition before this small window of opportunity passes us by. Conversely, proponents argue there is a moral imperative to develop these weapons as quickly as possible, to achieve greater compliance with international humanitarian law. While both arguments are defensible, the author considers the answer is found in the middle of these positions. A set of soft law guidelines recognises the reality that, in the current international context, a prohibition or strict new regulations are extremely unlikely to occur. Yet, soft law guidelines can assist to mitigate the very real risks that autonomous weapons will raise. The guidelines proposed by this dissertation will build upon those agreed at the meetings of the Group of Governmental Experts and will seek to balance risk mitigation, with widespread acceptance.

Word length:

The text of this dissertation, including cover page, table of contents, footnotes and bibliography, comprises approximately 32,433 words.

I Introduction

Autonomous weapon systems ("**AWS**") have been described as the third revolution in warfare, after gunpowder and nuclear arms.[1] The rapid development of these weapons has resulted in a number of parties joining the debate on whether AWS can comply with international humanitarian law ("**IHL**") and whether the significant risks raised by these weapons means we need to immediately prohibit their development and use. Conversely, others are arguing the critics' claims are misplaced and there is actually a moral imperative to develop these weapons to best ensure compliance with IHL.[2] Given the potential impacts of AWS, the stakes for this debate could not be higher. It is this dilemma that this dissertation seeks to address. In the current international context, what is the most realistic and pragmatic solution for addressing the challenges raised by AWS?

An AWS is the combination of a platform, a firing system and the artificial intelligence ("**AI**") that allows this weapon to operate. Given the risks that these weapons raise and the speed at which they are being developed, there are growing calls that the window for preventative action is fast closing[3] and we need an immediate prohibition, "before it is all too late".[4] New Zealand has stated on the international stage that when it comes to AWS, "standing still would effectively be a step backwards."[5] Yet, despite years of informal and formal discussions, international agreement on many issues in the AWS field is still far from being achieved. This has led to some parties claiming that the international discussions are purely a distraction, designed to placate civil society rather than actually address any challenges created by these new weapons.[6] On the other hand, some states and scholars are arguing the critics' claims are overstated and misplaced.[7] Instead, the existing IHL regime is sufficient to address these challenges. Not only *can* AWS comply with this IHL regime, but AWS' development and use may actually *increase* compliance with IHL. On this basis, there may be a moral imperative to develop these weapons as quickly as possible.

---

[1] Bonnie Docherty "Heed the Call: A Moral and Legal Imperative to Ban Killer Robots" (August 2018) Human Rights Watch <www.hrw.org> at 7.
[2] See "Working Paper of the Russian Federation: National Implementation of the Guiding Principles on Emerging Technologies in the Area of Lethal Autonomous Weapon Systems" (Paper submitted to the Group of Governmental Experts, Geneva, 2020) [Russia 2021 Working Paper]; and Michael N Schmitt and Jeffrey S Thurnher ""Out of the Loop": Autonomous Weapon Systems and the Law of Armed Conflict" (2013) 4 Harvard National Security Journal 231.
[3] "ICRC commentary on the 'Guiding Principles' of the CCW GGE on 'Lethal Autonomous Weapon Systems'" (paper submitted to the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, July 2020) at 4 [ICRC Commentary].
[4] Bonnie Docherty "Making the Case: The dangers of killer robots and the need for a pre-emptive ban" (December 2016) Human Rights Watch <www.hrw.org> at 2.
[5] "New Zealand Statement on Lethal Autonomous Weapons Systems" (paper submitted to the Meeting of High Contracting Parties on the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, Geneva, 2018).
[6] "Minority of states delay effort to ban killer robots" (29 March 2019) Campaign to Stop Killer Robots <www.stopkillerrobots.org> [States Delay Efforts].
[7] Russia 2021 Working Paper, above n 2; and Schmitt and Thurnher, above n 2.

What has further complicated this picture, is that several states with advanced militaries and significant international power have made it clear that they have no interest in participating in any work aimed at producing a new treaty, a political declaration or any other new measures that would regulate how these systems are developed, deployed or used. Instead, existing IHL is sufficient to appropriately ensure compliance with the law. Problematically for the critics of AWS, several of these states are countries that are either currently, or are likely to, develop this technology and the resulting weapon systems.

This leaves us in a dilemma. Are we stuck in an international stalemate, held hostage by a small collection of large states who are preventing us from being able to address the ever-increasing challenges raised by AWS? Or is much of this debate just well-intended hype, being blown out of proportion and preventing the development of weapons that may actually increase compliance with IHL? This dissertation seeks to forge a pathway down the middle of these two opposing positions. Primarily, it seeks to answer the central question of, in the current international context, what is the most realistic and pragmatic solution for addressing the challenges raised by AWS. Unlike other works in this field, this dissertation attempts to examine not only the legal mechanism that is most likely to be adopted, but also the content of such a legal mechanism.

Given the significant breadth of the AWS field, there are issues that this dissertation will need to address, but is unable to examine in depth or ultimately answer. This includes how these systems should be characterised and defined, how AI influences weapon systems, what these weapon systems may one day become and whether these future systems will be able to comply with IHL.

In order to answer this dissertation's central question, we will first briefly examine what an autonomous weapon system is. We will then look at the current international context, including the role that New Zealand has played, before considering whether AWS can comply with the existing IHL regime. In light of this context, this dissertation will consider what options are available to address the risks raised by AWS. This includes implementing legal mechanisms via the Convention on Conventional Weapons'[8] ("**CCW**") Group of Governmental Experts ("**GGE**"), adding a new protocol to the CCW or negotiating an entirely new treaty on AWS.

Lastly, we will seek to find a pragmatic solution to the dissertation's central question. In light of the current international context, this dissertation proposes a soft law solution. More specifically, it recommends adding to the existing set of guidelines that the GGE has currently negotiated. These guidelines will attempt to mitigate the risks created by AWS, while still being acceptable to a majority of states. This is no simple task, as a set of guidelines that are too broad or too high level, risk adding minimal value to any challenges raised. On the other hand, well

[8] Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects 1342 UNTS 137 (opened for signature 10 October 1988, entered into force 2 December 1983).

intentioned guidelines that will not be accepted by the states currently developing these weapons, will also be of limited value. While it is a difficult path to tread, in the author's view, a soft law solution is the most realistic and pragmatic solution to the current stalemate we find ourselves in.

II What are Autonomous Weapon Systems?

Weapon systems, in their various forms, are as old as humanity itself; and the longer humans have lived on earth, the more sophisticated these weapons have become. AWS will be the latest embodiment of this on-going evolution.

Yet, for the first time, this latest incarnation of weaponry may completely remove human involvement from the weapon's critical inputs. These, and other risks, have resulted in increasing calls for a pre-emptive ban of this technology before it reaches the battlefield. Human Rights Watch, for example, states a ban should be implemented as soon as possible, before this revolutionary and dangerous technology enters military arsenals.[9] Conversely, states such as the United States and Russia are rejecting these calls for a prohibition and are strongly opposed to any work aimed at a new treaty, political declaration, or any other new measures.[10] Rather, they argue, these systems should be developed so they can enhance compliance with IHL.

Yet, before this debate can be engaged, we must first establish what AWS are. This is made particularly complex when one considers that autonomy in weapon systems has been steadily increasing over the past 50 to 100 years. Depending on how one characterises and defines AWS, they are either currently operating on the battlefields today or may never be developed.

A Characterising and Defining AWS

Exactly how AWS should be characterised and defined has been hotly debated for many years. Whether a machine is autonomous (either fully or partially), automated or automatic potentially impacts how much that machine can comply with IHL. Yet, despite significant discussion, there is no internationally agreed definition of what constitutes "autonomy" and how it should be classified within weapon systems.

Much of the discussion to date has surrounded three broad ways to characterise and define AWS: via the human-machine relationship, via the machine's decision-making process and the types of decisions or functions that are being made autonomous. In all of these definitions, it is important to remember that there is human involvement in at least some part of the process,

[9] Docherty, above n 4, at 2.
[10] States Delay Efforts, above n 6; and "Minority of states block progress on regulating killer robots" (4 September 2018) United Nations Association UK <www.una.org.uk> [States Block Progress].

whether it be initially programming the machine, deciding to deploy it or operating some of that machine's functions.

1 The human-machine relationship

Autonomy, via this first method of classification, is characterised and defined via a human's involvement in the machine's critical inputs. Critical inputs include the decisions to identify, select and engage a particular target.

On this basis, humans are either in-the-loop, on-the-loop or out-of-the-loop. A human operator in an "in-the-loop" system would make the decision to identify, select and engage a particular target. With an on-the-loop system, the weapon system has been programmed so that it can identify, select and engage a target independently of any human intervention, but a human has the ability to intervene and override or shut down that weapon system. Thirdly, an out-of-the-loop system has been programmed with algorithms and AI to identify, select and engage a target independently of any human intervention. An out-of-the-loop system would be considered a fully autonomous weapon system.

The United States uses the human-machine relationship to define AWS:[11]

> A weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation.

Norway, Austria, New Zealand and The Human Rights Watch share similar human-machine relationship definitions.[12]

2 The machine's decision-making process

Autonomy can also be classified by the ability of a system to exercise control over its own behaviour or decisions and deal with uncertain or unforeseen environments. The NATO Industrial Advisory Group ("**NIAG**")[13] sets this out in a four-tier "level" system, as shown in the following table 1.[14] A level four system would be considered a fully autonomous weapon system.

---

[11] United States Department of Defense "Autonomy in Weapon Systems" (21 November 2012, updated 8 May 2017) Directive 3000.09 at 13 [DoD Directive].
[12] Daan Kayser and Stepan Denk "Keeping Control: European positions on lethal autonomous weapon systems" (12 November 2017) PAX for Peace <www.paxforpeace.nl> at 7.
[13] The NIAG is a high-level consultative and advisory body of senior industrialists of NATO member countries.
[14] "Pre-Feasibility Study on UAV Autonomous Operations" (NATO Industrial Advisory Group Study Group 75, study paper of the NATO Industrial Advisory Group, 2004) at 14-15.

Table 1:

Level	Degree of the machine's ability to exercise control over its own critical operating functions
Level 1: Remotely controlled system	The system's behaviour and actions depend on the human operator's inputs. The human operator makes the decision to identify, select and engage a particular target.
Level 2: Automated system	The system's behaviour and actions depend on pre-programmed functionality. The weapon system reacts in predefined procedures to specific pre-programmed parameters or sensory input, such as an approaching missile.
Level 3: Autonomous non-learning System	The system's behaviour and actions are driven by fixed rules, which dictate specific goal driven reactions or behaviours. As it is a non-learning system, there are limitations to the environments is can operate predictably or reliably within.
Level 4: Autonomous self-learning system	A system that continually self-improves and modifies its behaviour from a set of governing rules. This "goal-oriented" behaviour allows the weapon to create or modify rules based on previous experience. Theoretically, these weapon systems are capable of operating in environments that were not foreseen or specifically programmed in the design stage.

The United Kingdom uses the machine's decision-making process to define AWS: "[M]achines with the ability to understand higher-level intent, being capable of deciding a course of action without depending on human oversight and control."[15] A human will, of course, be required to initially programme that machine, but once programmed it is capable of deciding its own course of action. Interestingly, using this definition, the United Kingdom believes that "LAWS do not, and may never, exist" and "the UK considers that existing highly automated weapons are not, and should not, be part of this [AWS] discussion."[16]

3 The types of decisions or functions being made autonomous

The third broad category classifies autonomy by the types of decisions or functions that a weapon system autonomously makes. Some decisions can be made without presenting ethical

[15] British Ministry of Defence "Unmanned Aircraft Systems" (August 2017) Joint Doctrine Publication 0.30.2 at 13.

[16] "Statement to the Informal Meeting of Experts on Lethal Autonomous Weapon Systems" (United Kingdom of Great Britain and Northern Ireland Statement to the Informal Meeting of Experts on Lethal Autonomous Weapon Systems, 11-15 April 2016) [UK Statement to IME].

or legal risks (such as the ability to autonomously land), while others provide much greater concern (such as the ability to identify, select and engage targets without human involvement).

The International Committee of the Red Cross ("**ICRC**") has defined AWS via this third classification:[17]

> After initial activation by humans, taking the role of processes that are ordinarily controlled by humans, such that they can independently select (including searching for, identifying, detecting and selecting) and attack (including the use of force against, neutralisation and destruction) targets without any human intervention.

While the above broad categories capture much of the characterisation and definition debate, there are other ways to classify "autonomy" too. For example, explaining autonomy via whether the machine is lethal or non-lethal or the extent of that system's self-governance.[18] Others have combined these approaches, such as China, which adopted a definition that combines various aspects of the above definitions.[19]

In practice, the Stockholm International Peace Research Institute ("**SIPRI**")[20] has noted that it has proved difficult to measure, and therefore determine, which of the categories many systems fall within.[21] A full understanding of what constitutes "autonomy" and how it should be defined is, therefore, still some way off.

B The Current Limits of Autonomous Weapon Systems' Technology

As there has been an inability to reach an international consensus on both the characteristics and definitions of AWS, an argument regularly put forward is that calls to impose any new regulations or prohibitions are premature.[22] The argument follows that creating strict new regulations or a prohibition at this stage is too speculatory and may just create solutions to issues that will never in practice become problems. Alternatively, any regulations created with limited understanding of AWS technology may simply be bypassed or have significant loopholes. Accordingly, before we can address solutions, we must first briefly examine the technological limits of AWS.

---

[17] "International humanitarian law and the challenges of contemporary armed conflicts: Report prepared for the 32nd International Conference of the Red Cross and Red Crescent" (ICRC report prepared for the 32nd International Conference of the Red Cross and Red Crescent, 8-10 December 2015) at 44.

[18] David Mindell *Our Robots, Ourselves: Robotics and the Myths of Autonomy* (Viking, New York, 2015) at 12.

[19] See Austin Wyatt "Charting great power progress toward a lethal autonomous weapon system demonstration point" (2020) 20 Defence Studies 1 at 2-3.

[20] SIPRI is an independent international institute dedicated to research into conflict, armaments, arms control and disarmament.

[21] Vincent Boulanin and Maaike Verbruggen "Mapping the Development of Autonomy in Weapon Systems" (November 2017) Stockholm International Peace Research Institute <www.sipri.org> at 6.

[22] Schmitt and Thurnher, above n 2, at 234; "Chairperson's Summary" (Chairperson's summary of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, 19 April 2021) at 20 [Chairperson's Summary]; and the positions of various European states in Kayser and Denk, above n 12, at 16-17.

At a fundamental level, technology operates via human programmers solving problems with mathematical rules and instructions that a computer can understand. More specifically, machines operate via sensors (which gather data about the world), hardware/software (that allows that system to understand that data and transform it into plans and actions), communication technology/actuators (which allow the machines to interact with humans and other machines) and end-effectors (which allow the systems to execute actions).[23]

A further underlying concept in autonomy is the ability of a computer system to "learn". Machines learn by computing statistical relationships in data. In order to "learn", they need to be provided with specific data relationship rules and a significant amount of data.[24] If this can be provided, programmers do not need to explicitly define every problem and solution. Rather, the machine improves its knowledge via its experience.

Presently, most software is still "handcrafted", such that programmers are required to define the various problems that the software is required to solve and craft the manner in which it will solve those problems.[25] This requires a significant amount of knowledge about the tasks that will be required of the weapons and the environments in which those weapons will operate. While machine learning is developing rapidly, there are still significant hurdles for programmers to overcome. It is thought that a "learning system" is unlikely to be developed and deployed in the near future.[26] Accordingly, for the foreseeable future, programmers will be required to handcraft software or use limited forms of machine learning. This will make it difficult for AWS to achieve reliable and predictable results in a range of complex environments.

Nevertheless, our understanding of this technology has still developed to a point that allows for discussions on AWS risk mitigation. This is comparable to the understanding of blinding laser weapons, which too had not been fully developed prior to international discussions and ultimately prohibition. Similar to those weapons, there has been significant international discussions on AWS and the potential risks that these weapons raise.

III The International Context

Despite many years of deliberations, relatively little has been agreed to on the international stage. This has led to claims that the discussions to date have purely been an exercise "to placate civil society, distract public attention, and manage media expectations rather than seriously

[23] Boulanin and Verbruggen, above n 21, at 11-12.
[24] At 16.
[25] At 16.
[26] Boulanin and Verbruggen, above n 21, at 17; Anna Bacciarelli "Artificial intelligence: the technology that threatens to overhaul our rights" (20 June 2017) Amnesty International <www.amnesty.org>; Hugo Klijn and Maaike Okano-Heijmans "Managing RAS: The Need for New Norms and Arms Control" (17 March 2020) The Hague Centre for Strategic Studies <www.hcss.nl> at 13; and Noel Sharkey "Saying 'No!' to Lethal Autonomous Targeting" (2010) 9 Journal of Military Ethics 369 at 378.

address the challenges they pose for humanity."[27] Klijn and Okano-Heijmans have doubted whether the international efforts to date, are sufficient.[28]

These criticisms are, in the author's view, unfair. As this Part will examine, international debate on the challenges raised by AWS has not occurred in a legal vacuum. On the contrary, there has been significant progress via the legal machinery created by the CCW. Yet, despite this progress, in the author's view, the current international context means a treaty prohibiting AWS or implementing strict new regulations is unlikely to occur in the near future.

A International Discussions via the CCW

Over the past several years, there have been various forums for discussions on AWS. The "Rio Seminar", convened by Brazil, and the "Berlin LAWS Forum", convened by Germany, informally discussed various topics on AWS in an attempt to share knowledge and understandings.[29] Webinars have also been convened jointly by the United Nations Institute for Disarmament Research and the United Nations Office for Disarmament Affairs with similar objectives.[30]

The main discussions on AWS have, however, taken place via the framework established by the CCW. The CCW, which entered into force in 1983, was negotiated under the auspices of the United Nations and builds upon long-established customary IHL principles.[31]

The CCW is a particularly useful treaty in the IHL context as it provides a framework to amend current protocols or create new protocols in response to the development of new weapons. The CCW only contained three protocols when it was originally adopted in 1980 and has since had two additional protocols added to it and amendments made to the original protocols.

States that are parties to the CCW meet annually to review the operation of the CCW and can establish meetings of governmental experts to consider new issues appropriate for regulation under the CCW.[32] It is at these meetings that it has been agreed that the CCW is an appropriate mechanism to be discussing the challenges raised by AWS.[33]

---

[27] States Delay Efforts, above n 6; and States Block Progress, above n 10. For general discussion on the difficulty of regulating AWS see Frank Sauer "Stepping back from the brink: Why multilateral regulation of autonomy in weapons systems is difficult, yet imperative and feasible" (2020) 102 International Review of the Red Cross 235.
[28] Klijn and Okano-Heijmans, above n 26, at 9.
[29] Chairperson's Summary, above n 22, at 3.
[30] At 3.
[31] "Additional Protocol to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects: Text with amendments and protocols adopted through 28 November 2003" (June 2005) International Committee of the Red Cross <www.icrc.org> at 6.
[32] At 5.
[33] "Report of the 2019 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems" (final report of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, 25 September 2019) guiding principle (k) at 13 [2019 GGE Report].

B The Group of Governmental Experts on Autonomous Weapon Systems

Under the CCW framework, an informal "meeting of experts" was established in 2014 to discuss the questions related to emerging technologies in the area of AWS.[34] These discussions covered various issues such as the technicalities and characteristics of AWS and their compliance with IHL.

It was decided at the 2016 meeting of experts to establish a group of governmental experts to "explore and agree on possible recommendations on options related to emerging technologies in the area of lethal AWS…".[35] The GGE operates by conducting its work and adopting, by consensus, a final report. This report is then submitted to a meeting of the high contracting parties of the CCW for acceptance (again by consensus). The rules of procedure that operate for the CCW, are equally applicable for the GGE meetings.[36]

The GGE met to discuss AWS in 2017, 2018 and 2019. Further meetings were scheduled for 2020 and 2021 but have been impacted by the Covid-19 pandemic. Instead, states have submitted working papers on various AWS topics until they are again able to meet.

The central topics for discussion at the GGE meetings have remained relatively static over the past several GGE meetings, covering topics such as potential challenges posed by AWS, the human element in AWS and possible options for addressing humanitarian and international security challenges posed by AWS.[37] This last topic examined what can be done to ensure compliance with IHL and responsibility for decisions on the use of weapons and force. The options put forward ranged from a legally binding instrument at one end of the spectrum, to a mere recognition that IHL adequately addresses AWS and no further discussions are required. While certain states have been less constructive than others, there has been little support for a position that no further discussions on AWS are needed.[38]

While some critics have argued to the contrary[39], the GGE meetings have resulted in some tangible outcomes. In 2019, eleven guiding principles on AWS were adopted by consensus by the high contracting parties of the CCW.[40] These guidelines cover a broad range of issues, including the applicability of IHL to AWS. The specific content of the GGE guiding principles is discussed in greater detail below.

---

[34] "2014 Meeting of Experts on Lethal Autonomous Weapons Systems" (2014) United Nations <www.unog.ch>.
[35] "Recommendations to the 2016 Review Conference" (working paper to the Informal Meeting of Experts, Geneva, December 2016).
[36] 2019 GGE Report, above n 33, at 1.
[37] 2019 GGE Report, above n 33, at 3.
[38] Alice Beck, Daan Kayser and Frank Slijper "State of AI, Artificial Intelligence, the military and increasingly autonomous weapons" (April 2019) PAX for Peace <www.paxforpeace.nl> at 17.
[39] Klijn and Okano-Heijmans, above n 26, at 9; and Richard Moyes "Autonomy in weapons systems – considering approaches to regulation" (March 2020) Article 36 <www.article36.org>.
[40] 2019 GGE Report, above n 33, at 7.

These guiding principles provide a significant step forward for the international discussions on AWS. They have not, however, been without criticism. There are questions of how they will be implemented, operationalised and, as noted by the chair of the GGE meetings, parties are likely to have different interpretations of the guidelines.[41] This, in the author's view, threatens to undermine their effectiveness as a state could interpret them to fit their particular stance on AWS (either for or against). As the following sections set out, unfortunately, it is also unlikely that there will be an international consensus on many of these issues any time soon.

C A Growing Call to Prohibit or Strictly Regulate AWS

As the international discussions have progressed, there have been growing calls to immediately address the significant risks that AWS pose. At the top of critics' list of proposed options, is a legally binding instrument. Such an instrument could take the form of either a completely new negotiated treaty or, under the process described above, a new protocol could be added to the CCW. As we might expect, various states such as Austria, Brazil and Chile have been leading these calls.[42] Yet, as seen with other weapon technologies, a growing number of non-governmental organisations and private entities have joined the call to prohibit these weapons.

To date, there have been a dedicated but small number of states that are advocating for a legally binding instrument to prohibit AWS' development and use. For example, Austria, Brazil and Chile submitted a proposal at the 2018 GGE meeting which sought a mandate to negotiate a legally binding instrument.[43] In support of this, 30 states, as at August 2020, have called for a legally binding instrument to prohibit AWS.[44] China has called for a prohibition on the "use" of AWS, however, unsurprisingly, has not extended this to the development or manufacture of AWS.[45] Rather than a full prohibition, some states are calling for strict new regulations to ensure that AWS can comply with IHL.[46]

It is not just states that have been calling for a prohibition either. UN Secretary-General Antonio Guterres has also called for a prohibition, stating in November 2018: "I call upon States to ban these weapons, which are politically unacceptable and morally repugnant."[47] The European Parliament and the Organization for Security and Co-operation in Europe have taken similar

---

[41] "Non-paper by the GGE Chair" (working paper to the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, March 2020) at 1.
[42] "Stopping Killer Robots: Country Positions on Banning Fully Autonomous Weapons and Retaining Human Control" (10 August 2020) Campaign to Stop Killer Robots <www.stopkillerrobots.org> at 4 [Country Positions].
[43] "Proposal for a Mandate to Negotiate a Legally binding Instrument that addresses the Legal, Humanitarian and Ethical Concerns posed by Emerging Technologies in the Area of Lethal Autonomous Weapons Systems" (working paper to the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, 30 August 2018).
[44] States Delay Efforts, above n 6; and Country Positions, above n 42, at 4.
[45] Country Positions, above n 42, at 4.
[46] Including the Czech Republic, India, Ireland and South Africa, Country Positions, above n 42.
[47] "Autonomous weapons that kill must be banned, insists UN chief" (25 March 2019) United Nations <www.news.un.org> [AWS must be banned].

positions.[48] The ICRC finally stated its position on AWS in 2021, recommending new legally binding rules to ensure compliance with IHL.[49]

Similar to what occurred prior to the treaties on cluster munitions and anti-personnel mines, various non-governmental organisations have also joined the growing calls to prohibit AWS. PAX, Human Rights Watch, Article 36, Amnesty International, The International Committee for Robot Arms Control ("**ICRAC**") and the Campaign to Stop Killer Robots, to name just a few, are rallying behind the call to prohibit AWS.[50] Concerned that the risks of AWS may not be adequately addressed by states alone, many of these organisations have been actively involved in the international discussions. Several of these organisations submitted papers to the GGE in 2020 and 2021.

Various organisations in the private sector have also joined the debate. Several companies and organisations have agreed to not develop the AI for AWS. This includes Elon Musk, Google DeepMind's founders and CEOs of various robotics companies.[51] While not always necessarily advocating for a prohibition, a number of scholars and advocates have raised significant concerns that AWS may pose to IHL, ethics, morals, operationally, as well as wider concerns such as the impact on international stability. This includes Elvira Rosert and Frank Sauer, Mary Wareham and John Lewis (amongst many others).[52] One leading scholar in this field, Noel Sharkey, has categorically stated "a robot should never be delegated with the decision to apply violent force".[53]

There is, therefore, a growing coalition of states, organisations and scholars throwing their support behind strictly regulating or negotiating a legally binding instrument to prohibit the development and use of AWS. Critically, however, the environment is very different from that of other weapon technologies, prior to instruments being entered into to address the risks with those technologies.

Mostly notably, several states with advanced militaries and significant international power have attempted to shut down the conversation on such a legally binding instrument. Five states, including Australia, Israel, Russia, South Korea, and the United States, have stated that they

---

[48] "Organisation for Security and Cooperation in Europe: Annual Report 2018" (2018) Organisation for Security and Cooperation in Europe <www.osce.org>; "Report on a European Parliament recommendation to the Council on the 73rd session of the United Nations General Assembly (2018/2040(INI))" (27 June 2018) European Parliament <www.europarl.europa.eu>.

[49] "ICRC position on autonomous weapon systems" (12 May 2021) International Committee of the Red Cross <www.icrc.org>.

[50] Other organisations in this debate include the UN Institute for Disarmament Research, Nobel Women's Initiative, Association for Aid and Relief and the Women's International League for Peace and Freedom.

[51] "All action and achievements" (undated) Campaign to Stop Killer Robots <www.stopkillerrobots.org>.

[52] See Elvira Rosert and Frank Sauer "Prohibiting Autonomous Weapons: Put Human Dignity First" (2019) 10 Global Policy 370; Mary Wareham "Statement by the Campaign to Stop Killer Robots to the Convention on Conventional Weapons" (22 November 2018) Human Rights Watch <www.hrw.org>; and John Lewis "The Case for Regulating Fully Autonomous Weapons" (2015) 124 The Yale Law Journal 1309.

[53] Noel Sharkey "Why robots should not be delegated with the decision to kill" (2017) 29 Connection Science 177 at 178.

"strongly opposed any work aimed at a new treaty, political declaration, or any other new measures."[54] Russia unequivocally stated it "would adhere to no international ban, moratorium or regulation on such weapons."[55] Three other states, including Israel, France and Turkey, have expressed a firm opposition to support negotiating a new treaty prohibiting AWS.[56] The author is unaware of any advocacy groups or organisations similarly attempting to shut down the conversation on prohibiting AWS, however, it is unsurprising to note that various manufacturers and military experts in this field are touting the significant benefits that will result from AWS.[57]

The positions of these states are not made in a legal vacuum, absent any consideration of international law. On the contrary, as examined in Part IV, these states argue that not only can AWS comply with IHL, but they may even *enhance* compliance. In furtherance of this view and the significant military utility that these machines will produce, these states have been investing significant time and money into the development of the technology underlying AWS.

D International Efforts to Develop AWS

In September 2017, President Vladimir Putin stated on national television that "[a]rtificial intelligence is not only the future of Russia, it is the future of all mankind" and "[a]nyone who becomes a leader in this field will be the ruler of the world."[58] Never one to be outdone, President Trump stated in 2020 that the United States was currently producing a "super-duper missile".[59] This shows the importance that these states are placing on developing these emerging technologies as quickly as possible.

The United States is said to be the world leader in AI, largely due to the significant number of tech companies based there (including Google, Microsoft, Amazon, Facebook and Apple).[60] The United States is attempting to leverage this AI advantage to benefit its military. In 2016, then Deputy Secretary of Defence Bob Work noted, the Third Offset's[61] aim:[62]

---

[54] States Delay Efforts, above n 6; and States Block Progress, above n 10.
[55] Patrick Tucker "Russia to the United Nations: Don't Try to Stop Us From Building Killer Robots" (21 November 2017) Defence One <www.defenseone.com>.
[56] "Country Views on Killer Robots" (25 October 2019) Campaign to Stop Killer Robots <www.stopkillerrobots.org>.
[57] See "Airpower Teaming System" (2021) Boeing <www.boeing.com>; and Amitai Etzioni and Oren Etzioni "Pros and Cons of Autonomous Weapons Systems" (May-June 2017) 97 Military Review 72 at 72-74.
[58] "Open lesson "Russia, aspiring to the future"" (1 September 2017) President of Russia <www.kremlin.ru> [President of Russia].
[59] Kyle Mizokami "Trump's 'Super Duper Missile' Is Actually Super Duper Real" (20 July 2020) Popular Mechanics <www.popularmechanics.com>.
[60] Beck, Kayser and Slijper, above n 38, at 6.
[61] The "Third Offset Strategy" seeks to outmanoeuvre advantages made by top adversaries through technology. Beck, Kayser and Slijper, above n 38, at 6; and Wyatt, above n 19, at 4-5.
[62] Beck, Kayser and Slijper, above n 38, at 6.

> …is to exploit all advances in AI and autonomy and insert them into the Department of Defence's battle networks to achieve a step increase in performance that the department believes will strengthen conventional deterrence.

More recently, a United States Government-appointed panel in March 2021 recommended that not only should AWS not be banned, but "[w]e must adopt AI to change the way we defend America, deter adversaries, use intelligence to make sense of the world, and fight and win wars."[63]

To retain its lead in developing AWS, the 2020 Department of Defence budget set aside US$3.7b for autonomous systems and US$927m for AI.[64] Were this not motivation enough, the United States is also very aware of the development of these weapons by other states. In a 2019 defence primer, the Congressional Research Service[65] noted that the United States may be compelled to develop AWS if the United States' adversaries do so.[66]

Not to be outdone, China too is seeking to develop the technology underlying AWS as quickly as possible. By 2030, China has committed to making "artificial intelligence theory, technology and application achieve the world's leading level to be the major artificial intelligence innovation centre of the world…"[67] In 2017, "48 per cent of total equity funding of AI start-ups globally came from China, compared to 38 per cent funded by the US, and 13 per cent by the rest of the world".[68] Commentators have also acknowledged China's covert attempts at developing AWS' technology, via intellectual property theft and industrial espionage.[69]

The United Kingdom and Russia also have ambitious technology plans too.[70] Russia, for example, is currently developing the Status-6 nuclear autonomous torpedo[71] and, in early 2020, Australia was testing a fighter jet with autonomous features with the purpose of creating cheap, expendable fighters to potentially provide "combat mass" to overload the enemy.[72]

---

[63] Eric Schmidt and others "Final Report: National Security Commission on Artificial Intelligence" (March 2021) National Security Commission on Artificial Intelligence <www.nscai.gov>.

[64] "The FY 2020 Budget Request: Security R&D" (23 April 2019) American Association for the Advancement of Science <www.aaas.org>.

[65] The Congressional Research Service serves as nonpartisan shared staff to congressional committees and Members of the United States Congress.

[66] Kelley M Sayler "Defence Primer: U.S. Policy on Lethal Autonomous Weapon Systems" (19 December 2019) Congressional Research Service <www.crsreports.congress.gov>.

[67] "Notice of the State Council Issuing the New Generation of Artificial Intelligence Development Plan" (July 2017) The Foundation for Law and International Affairs <www.flia.org>.

[68] Pablo Robles "China plans to be a world leader in Artificial Intelligence by 2030" (1 October 2018) South China Morning Post <www.scmp.com>.

[69] Ted Piccone "How can international law regulate autonomous weapons?" (10 April 2018) Brookings <www.brookings.edu>.

[70] Beck, Kayser and Slijper, above n 38, at 16 to 22.

[71] Franz-Stefan Gady "Russia's New Nuclear Torpedo-Carrying Sub to Begin Sea Trials in June 2020" (10 September 2019) The Diplomat <www.thediplomat.com>.

[72] Ewen Levick "Boeing's Autonomous Fighter Jet Will Fly Over the Australian Outback" (2020) IEEE Spectrum <www.spectrum.ieee.org>.

In late 2020, the world watched as Azerbaijan and Armenia engaged in a brief and brutal conflict. Approximately six weeks after this conflict started, Armenia signed a cease fire on "punishing terms."[73] The devastating efficiency of Azerbaijan's drones, many of which had significant amounts of autonomy[74], over traditional weapons such as tanks, was not only clear to see but was described as a game changer.[75] While not fully autonomous weapons, the efficiency and effectiveness of the autonomy on the battlefield would have been eagerly noted by powers across the world.

These examples illustrate the significant time, money and effort that is being expended to develop and master the AI required to create AWS. In light of these commitments, it is little wonder that the five states opposing a new treaty, political declaration, or any other new measures have taken the positions they have.

The stance of the states opposing treaties or other measures to mitigate the risks of AWS has led to intense criticism from critics, who argue measures such as those agreed at the GGE are both not enough and are not truly addressing the challenges that AWS pose to humanity.[76] Another organisation has stated that working solely on creating "guiding principles" has created a sense of collective action and engagement, but can serve to perpetually avoid the key issues.[77]

Yet the actions of these states are not made in ignorance of the current IHL regime. While scholars have raised concerns with AWS' ability to comply with certain aspects of IHL[78], such as distinction and proportionality, as examined in Part IV below, there are strong arguments that, in the right environments, AWS can not only comply with IHL but may actually *improve* compliance with IHL. At the extreme end of this argument, Anderson argues that there may even be "an affirmative moral obligation" to research and develop automation, robotics and AI technologies to better benefit IHL.[79] Umbrello, Torres and Bellis share similar views.[80] A United States government-appointed panel similarly agreed there was a moral imperative to

[73] Robyn Dixon "Azerbaijan's drones owned the battlefield in Nagorno-Karabakh - and showed future of warfare" (11 November 2020) The Washington Post <www.washingtonpost.com>.
[74] Such as the Israeli "Harop loitering munitions", Paul Iddon "The Last Azerbaijan-Armenia War Changed How Small Nations Fight Modern Battles" (25 March 2021) Forbes <www.forbes.com>. For the autonomy in the Harop weapon system see Boulanin and Verbruggen, above n 21, at 53-54.
[75] Dixon, above n 73; Daniel Edelstein "Potential Gains for Israel After Azerbaijan's Victory in Nagorno-Karabakh" (10 March 2021) Just Security <www.justsecurity.org>; and Iddon, above n 74.
[76] States Delay Efforts, above n 6; and Klijn and Okano-Heijmans, above n 26, at 9.
[77] Moyes, above n 39.
[78] Sharkey, above n 53; and Vincent Boulanin, Laura Bruun and Netta Goussac "Autonomous Weapon Systems and International Humanitarian Law" (June 2021) Stockholm International Peace Research Institute <www.sipri.org>.
[79] Kenneth Anderson "Why the Hurry to Regulate Autonomous Weapon Systems – But Not Cyber Weapons" (2016) 30 Temp Int'l & Comp L.J. 17 at 22.
[80] Angelo Bellis, Phil Torres and Steven Umbrello "The future of war: could lethal autonomous weapons make conflict more ethical?" (6 February 2019) 35 AI and Society 273 at 277.

investigate these AWS benefits.[81] As with any moral debate, however, there are just as many critics suggesting using AWS at all is morally repugnant.[82]

E New Zealand's Participation at the GGE Meetings

Before examining the ability of AWS to comply with IHL, it is first worth considering what role New Zealand has played within the AWS debate. New Zealand, as a party to the CCW, has participated in the various CCW and GGE meetings.[83]

While its early contributions welcomed the opportunity to join the discussion, New Zealand did not initially take a position on any particular issue.[84] Throughout the years, however, New Zealand's views on AWS have begun to crystalise.[85]

New Zealand has expressed a firm view that it has concerns on the legal, ethical and human rights challenges raised by AWS.[86] Further, it has stated that all AWS must comply with IHL, and has favoured a compliance-based approach to AWS.[87] This means the central question should be whether AWS can comply with IHL. New Zealand has stated that only humans should have control over a machine's critical functions and has consequently placed significant focus on ensuring there is meaningful human control in AWS.[88]

Human control should, therefore, play a central role in any definition of AWS and any accompanying compliance framework. New Zealand was a contributor, along with nine other states, in a paper provided to the GGE in 2020 providing commentary on the implementation of the eleven agreed guiding principles (discussed in greater detail below).[89] New Zealand proposed an operational framework with certain requirements of human control.[90]

---

[81] "US has 'moral imperative' to develop AI weapons, says panel" (26 January 2021) The Guardian <www.theguardian.com>.
[82] See AWS must be banned, above n 47; Docherty, above n 1; Sharkey, above n 53, at 181; Richard Moyes "Critical Commentary on the "Guiding Principles"" (November 2019) Article 36 <www.article36.org> at 3.
[83] "High contracting parties and signatories" (17 June 2020) United Nations <www.unog.ch>.
[84] Joseph Ballard "Statement by Joseph Ballard Deputy Permanent Representative to the Conference on Disarmament" (New Zealand Statement to the Informal Meeting of Experts on Lethal Autonomous Weapon Systems, Geneva, 13 May 2014).
[85] See Hon Phil Twyford "Workshop on Lethal Autonomous Weapons Systems - opening remarks" (14 April 2021) The Beehive <www.beehive.govt.nz>.
[86] Letter from Winston Peters (Minister of Foreign Affairs) to Mary Wareham (Coordinator, Campaign to Stop Killer Robots) regarding New Zealand's position on LAWS (1 May 2019).
[87] Ballard, above n 84.
[88] Ballard, above n 84; "New Zealand Statement" (New Zealand Statement to the Meeting of Experts on Lethal Autonomous Weapon Systems, Geneva, 2016); and Katy Donnelly "Statement by Katy Donnelly Deputy Permanent Representative to the Conference on Disarmament, Geneva" (New Zealand Statement to the Group of Governmental Experts, Geneva, 13 April 2018).
[89] Including Austria, Belgium, Brazil, Chile, Ireland, Germany, Luxembourg, Mexico and New-Zealand. "Joint 'Commentary' on Guiding Principles A, B, C and D" (Paper submitted to the Group of Governmental Experts, Geneva, 2020) [Joint Commentary].
[90] Joint Commentary, above n 89.

New Zealand has also placed emphasis on weapon reviews under article 36 of 1977 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) ("**Additional Protocol I**")[91] and ensuring these reviews are robust enough that emerging weapons can be appropriately reviewed for compliance with IHL.

To implement the above views, New Zealand has suggested a political declaration would be appropriate.[92] This declaration "should set out key disciplines on the development and use of LAWS such as meaningful human control and the operational safeguards needed to ensure that."[93]

From a domestic perspective, New Zealand's Manual of Armed Forces Law does not specifically refer to autonomous weapon systems.[94] As indicated in statements by the Government, however, New Zealand has attempted to ensure that emerging technologies comply with IHL via the article 36 weapon review process.[95] The Manual of Armed Forces Law specifically provides that the principles of IHL apply to all potential technology available for military use, including robotic weapons and weapons with AI.[96]

IV Autonomous Weapon Systems and International Humanitarian Law

In 2019, Winston Peters, the then New Zealand Minister of Foreign Affairs, stated: "[o]ur view is that international law already sets limits on lethal AWS, notably through Additional Protocol 1 of the Geneva Conventions."[97] At the heart of the AWS debate, is whether these emerging weapon systems can comply with IHL, both now and in the future. If they can, then no new regulation or mechanism may be needed. If they cannot, these weapons may need pre-emptive prohibition. This Part examines whether the existing IHL regime can stretch and adapt to these emerging technologies.

A The Current IHL Regime as it Relates to AWS

The calls for AWS to either be prohibited or subject to strict new regulations are growing louder. Yet, there is already an existing IHL regime that applies to AWS. Poland, for example, acknowledged at the 2019 GGE Meeting that this existing regime may be all that is needed to

---

[91] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) 1125 UNTS 3 (opened for signature 8 June 1977, entered into force 7 December 1978), art 36.
[92] Peters, above n 86.
[93] "Agenda item 5(e)" (New Zealand Statement to the Group of Governmental Experts, Geneva, 27 March 2019).
[94] New Zealand Defence Force "Manual of Armed Forces Law: Commander's Handbook on Military Law DM 69 (2 ed) Volume 4 Law of Armed Conflict" (20 June 2020) [Defence Manual].
[95] Peters, above n 86.
[96] Defence Manual, above n 94, at 7.4.6.
[97] Peters, above n 86.

address AWS' challenges, noting: "We already have a legally binding instrument which is IHL".[98] The United Kingdom has also expressed similar sentiment, noting that existing IHL is sufficient to control and regulate AWS.[99]

IHL requires that a state that is intending to develop, acquire or use a new weapon technology evaluate two separate areas of law. Firstly, the state must determine whether the weapon itself is lawful "per se". This includes conducting a weapon review and ensuring that weapon does not have certain characteristics that make it inherently unlawful. Secondly, the state needs to establish whether the use of that weapon is prohibited.[100] This means ensuring that its use is conducted in accordance with the IHL's core principles of proportionality, distinction and precautions in attack.

1 Weapon reviews

In order to determine whether the development, purchase or use of a weapon system is lawful under IHL, a state legally obligated to undertake a weapons review. The ICRC submits this review applies to "weapons of all types"[101], which would, therefore, encompass AWS. This legal obligation requires all states to consider whether the development, acquisition or use of a new weapon or technology (including AWS) would, in some or all circumstances, breach the international rules that apply to that state.[102]

This is an express duty for those parties to Additional Protocol I. The ICRC, Dahl and Dinstein submit that even those parties not party to Additional Protocol I are subject to this legal obligation. The ICRC has stated that the "requirement that the legality of all new weapons, means and methods of warfare be systematically assessed is arguably one that applies to all States, regardless of whether or not they are party to Additional Protocol I".[103] Dinstein notes that those states not party to Additional Protocol I must determine whether the AWS' employment would, in some or all circumstances, be prohibited by applicable principles of IHL.[104] For those states subject to Additional Protocol I, and arguably all other states, the

---

[98] Alice Black and Daan Kayser "Convergence? European positions on lethal autonomous weapon systems Update 2019" (November 2019) PAX for Peace <www.paxforpeace.nl> at 16.
[99] Letter from Annabel Jenkin (Conventional Arms Policy Officer) to Natalie Samarasinghe and Richard Moyes (Executive directors, United Nations Association) regarding the United Kingdom's definition of lethal autonomous weapon systems (8 December 2017).
[100] Jeffrey S Thurnher "Means and Methods of the Future: Autonomous Weapon Systems" in Paul AL Ducheine, Michael N Schmitt and Frans PB Osinga (ed) "Targeting: The Challenges of Modern Warfare" (T.M.C. Asser Press, The Hague, 2016) 177 at 185.
[101] Kathleen Lawland "A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977" (December 2006) 88 International Review of the Red Cross 931 at 937.
[102] William H Boothby *New technologies and the law in war and peace* (Cambridge, Cambridge University Press, 2019) at 2.
[103] Lawland, above n 101, at 933.
[104] Yoram Dinstein and Arne Dahl "Remote and Autonomous Weapons" in Yoram Dinstein and Arne Dahl *Oslo Manual on Select Topics of the Law of Armed Conflict* (Springer International Publishing, Switzerland, 2020) at 39.

temporal application of a weapon review covers the weapon's study, development, acquisition and adoption, but not necessarily post acquisition/adoption unless that weapon undergoes further modification.[105] It is arguable whether, and the degree to which, a software update would require a new weapon review.[106] As it relates to the "means" of war, this duty is widely regarded as customary international law.[107]

There is no single model for compliance with weapons reviews and one government's model may not necessarily be appropriate for another.[108] So too should a state be wary of relying on another state's weapon review assessment.[109] Rather, the obligation is on each state to make its own assessment. Exactly how these weapon reviews will apply to AWS, both under current technology and possible future technology, is a hotly debated topic. Working papers, including papers from Australia in 2018 and 2019, have been submitted at the GGE meetings seeking to explore the challenges.[110] One commentator has stated that AWS in their current state would require an operator to be in-the-loop in order to comply with weapon reviews laws.[111] Yet, we already have various defensive "autonomous" weapons, such as the United States Navy's Close in Weapons System, with humans on-the-loop that have passed these weapons reviews.[112]

Given AWS will constitute new technologies, the weapon review will play a critical role in AWS' development. This dissertation will therefore return to these weapon reviews later, when considering whether additional guidelines can assist AWS to comply with this core IHL principle.

2 Development of weapons – is the weapon lawful "per se"?

[105] Lawland, above n 101, at 951-952.
[106] Boulanin, Bruun and Goussac, above n 78, at 32-33.
[107] Jean-Marie Henckaerts and Louise Doswald-Beck *ICRC Customary International Humanitarian Law Volume I: Rules* (Cambridge University Press, Cambridge, 2005) at 250; Kenneth Anderson, Daniel Reisner and Matthew Waxman "Adapting the Law of Armed Conflict to Autonomous Weapon Systems" (2014) 90 International Law Studies 386 at 398; Schmitt and Thurnher, above n 2, at 271.
[108] Gary D Solis *The Law of Armed Conflict: International Humanitarian Law in War* (2nd ed, Cambridge University Press, New York, 2016) at 751; and Boulanin, Bruun and Goussac, above n 78, at 9-10.
[109] Solis, above n 108, at 751.
[110] "The Australian Article 36 Review Process" (working paper to the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, 30 August 2018); and "Australia's System of Control and applications for Autonomous Weapon Systems" (working paper to the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, 20 March 2019).
[111] Peter Combe "Autonomous Doctrine: Operationalising the Law of Armed Conflict in the Employment of Lethal Autonomous Weapon Systems" (2020) 51 St. Mary's Law Journal 35 at 65.
[112] At 65.

The Brussels Declaration[113], the Hague Regulations of 1899 and 1907[114] and article 35(1) of Additional Protocol I acknowledge that the laws of war do not recognise in belligerents an unlimited power in the adoption of means of injuring the enemy. This means the right of the parties to choose methods or means of warfare are not unlimited. IHL has established the two following core principles that AWS will need to comply with to ensure they are not unlawful per se.

(a) Superfluous injury and unnecessary suffering

There is a prohibition on the use of means and methods of warfare which are of a nature to cause superfluous injury or unnecessary suffering. This is recognised in the Hague Regulations of 1907[115], article 35(2) of Additional Protocol I and is widely accepted as customary international law.[116] This principle is aimed at preventing combatants from being subjected to inhumane suffering which serves no military purpose.

To date, it has largely been AWS' "engagement" that has raised IHL compliance concerns (such as an AWS targeting humans without any human involvement). This IHL principle, however, pertains to the effect of the weapon, rather than the manner of that weapon's engagement.[117] As the autonomous features of a weapon system relate to its engagement, it is unlikely that AWS will prima facie contravene this principle.[118]

It is entirely possible that a particular weapon attached to an AWS could cause unnecessary suffering, contravening this IHL principle, but it would not be the autonomous features making this system illegal. AWS will not therefore require any additional programming, for example, to comply with this principle. The possibility of AWS containing a weapon that causes superfluous suffering, is not, in the author's opinion, a strong basis for a pre-emptive ban on the development or use of AWS.[119]

---

[113] Project of an International Declaration concerning the Laws and Customs of War (Brussels, 27 August 1874 (Brussels Declaration), art 12.
[114] Regulations Respecting the Laws and Customs of War on Land annexed, respectively, to Hague Convention II of 29 July 1899; and Convention Respecting the Laws and Customs of War on Land (Hague Convention IV) 205 CTS 277 (opened for signature 18 October 1907, entered into force 26 January 1910), art 22 [Hague Regulations].
[115] Hague Regulations, above n 114.
[116] Henckaerts and Doswald-Beck, above n 107, rule 71 at 244.
[117] Schmitt and Thurnher, above n 2, at 245; Rebecca Crootof "Regulating New Weapon Technologies" in Ronald T P Alcala and Eric Talbot Jensen (ed) "The Impact of Emerging Technologies on the Law of Armed Conflict" (Oxford University Press, New York, 2019) at 20; and Charles Trumbull IV "Autonomous Weapons: How existing law can regulate future weapons" (2020) 34 Emory International Law Review 533 at 555 and 557.
[118] Schmitt and Thurnher, above n 2, at 245; Kenneth Anderson and Matthew Waxman "Debating Autonomous Weapon Systems, their ethics, and their regulation under International Law" in Roger Brownsword, Eloise Scotford and Karen Yeung *The Oxford Handbook of Law, Regulation and Technology* (Oxford University Press, Oxford, July 2017) at 1105.
[119] See Anderson and Waxman, above n 118, at 1105; Schmitt and Thurnher, above n 2, at 245; and Trumbull, above n 117, at 557.

(b) Weapons that are indiscriminate by nature

There is a prohibition on weapons that are of a nature to be indiscriminate. This is recognised in article 51(4)(b) of Additional Protocol I and is widely accepted as customary international law.[120] This principle provides that the uses for which the weapon was designed or intended cannot be indiscriminate.[121] A related principle is captured in article 51(4)(c) of Additional Protocol I, which provides a weapon is prohibited if it has uncontrollable effects or where the effects of that weapon cannot be limited.[122]

Situations could certainly be envisaged where AWS could, in certain environments, act indiscriminately. AWS operating in closely confined urban areas, for example. Yet the focus of this customary international law is whether a weapon can be appropriately aimed, regardless of whether this aiming comes from a human or a machine.[123] An example often cited is biological weapons, which are indiscriminate as they can never distinguish between civilians or a military objective.[124] This principle is, therefore, concerned with the inherent nature of the weapon, not the weapon's use on a particular occasion.

It has been argued that AWS can actually *increase* compliance with IHL, such as by being more precise and thereby reducing the risks to civilians.[125] This capacity to be precise adds weight to the argument that AWS are not "indiscriminate" by nature. Provided AWS can be appropriately programmed so they can be aimed in at least *some* occasions in accordance with IHL (such as in the air, desert or sea, where there are minimal civilians), then AWS are unlikely to contravene this principle as they will not be "inherently" indiscriminate.[126] In the author's view, there is no strong basis for a pre-emptive ban on the development or use of AWS due to their inability to comply with this principle.

3 Use of weapons

Even if a weapon is not illegal per se, its use may still be prohibited under IHL. There are several fundamental IHL principles that determine whether AWS' use is prohibited.

(a) Distinction

[120] Henckaerts and Doswald-Beck, above n 107, rule 70 at 237.
[121] Anderson, Reisner and Waxman, above n 107, at 399; and Trumbull, above n 117, at 556.
[122] Boothby, above n 102, at 21.
[123] At 21.
[124] Boothby, above n 102, at 21; and Trumbull IV, above n 118, at 556.
[125] Thurnher, above n 100, at 195.
[126] Schmitt and Thurnher, above n 2, at 246; Trumbull, above n 117, at 557; and Anderson and Waxman, above n 118, at 1105.

On the battlefield, a combatant is required to use his or her reasonable judgement to distinguish between enemy combatants and civilians, as well as military and civilian objects.[127] This core principle has been codified in articles 48, 51(2) and 52(1) of Additional Protocol I and is generally accepted as customary international law.[128]

Many distinction assessments rely on context and the environment in which the weapon system operates will play a critical role. A computer's ability to accurately make a distinction assessment will, therefore, depend on the environment in which it is making that assessment. In areas where there are few civilians, such as naval battles, a computer may easily be able to make a distinction assessment. Yet, in any complex urban environment, it would be much more difficult for AWS to comply with the principle of distinction. This is because AWS will need to make complex distinctions such as between combatants and those that are hors de combat. If the AWS was unable to comply with the distinction principle, it would be unlawful to use that system. Each party to a conflict must respect, and ensure respect, for IHL, so the party using the AWS would have a legal obligation to not use that system in that situation.[129]

A number of scholars and states have argued that the assessments of distinction and proportionality are "uniquely human assessments."[130] While sophisticated systems will be able to distinguish a tank from a civilian truck, it is a much more difficult task to distinguish between combatants and civilians that are directly participating in hostilities. This is made even more complex when the enemy is purposely attempting to flout IHL, such as using civilians as human shields. These assessments, it is argued, require a human to make them.

Yet, there are also contrary arguments that technology will actually be able to increase the accuracy of these assessments. Technology, such as on-board sensors, can already recognise military objects by their speed, the type of propulsion, what the target is made from, the type of electronic emissions and communications it emits,[131] its shape or its heat signature.[132] Machines have also been shown to recognise human stress, without needing physical contact.[133] These are assessments that humans are unable to compete with. Technology also allows AWS to monitor targets for long periods of time (the Harpy, for example, can loiter in the air for up to 9 hours[134]), further increasing the likelihood of accurately distinguishing a military target from a civilian. At the edge of this technology, it may even be possible to

[127] Anderson, Reisner and Waxman, above n 107, at 401; Trumbull, above n 117, at 561; Combe, above n 111, at 45; Thurnher, above n 100, at 188; Boothby, above n 102, at 20; and Boulanin, Bruun and Goussac, above n 78, at 6-7.
[128] Henckaerts and Doswald-Beck, above n 107, rule 1 at 3.
[129] Henckaerts and Doswald-Beck, above n 107, rule 40 at 495.
[130] Docherty, above n 4, at 19; See also Joint Commentary, above n 89, at 1-2; "National commentaries on the 11 guiding principles – Comments by Italy" (Paper submitted to the Group of Governmental Experts, Geneva, 2020) at 2 [Comments by Italy]; and Boulanin, Bruun and Goussac, above n 78, at 19.
[131] Schmitt and Thurnher, above n 2, at 247.
[132] Solis, above n 108, at 539.
[133] Combe, above n 111, at 42.
[134] Boulanin and Verbruggen, above n 21, at 53.

digitally reconstruct what a person is seeing by measuring brain activity with magnetic resonance imaging technology.[135]

There appears to be little doubt that technology will eventually be able to outperform humans with certain aspects of the distinction assessment; if not its entirety. Yet, it is open to debate whether this is ethically or morally right. To address this, a topic that has received significant recent debate, including support from New Zealand[136], is that all AWS should have certain limits of meaningful human control imposed in either their development or use (or both). Such meaningful human control, it is argued, would ensure that the core distinction principle would be adhered to. This dissertation will return to this debate later, as, while it is uncontroversial that at least some level of human involvement is necessary in AWS, exactly what "meaningful human control" means and how this may impact the development of the technology underlying AWS is subject to considerable debate and disagreement.

While this distinction debate is far from settled, there is no general consensus that this principle will result in AWS being automatically unable to comply with IHL and therefore result in them being unlawful.

(b) Proportionality

The second core principle for the use of weapons is the principle of proportionality. This principle is codified in articles 51(5)(b) and 57(2)(a)(iii) of Additional Protocol I and is widely recognised as customary international law.[137] The principle of proportionality prohibits attacks where it may be expected to cause injury or loss of civilian life (or damage to civilian objects) which are excessive in relation to the concrete military advantage anticipated. This complex principle requires the reasonably anticipated military advantage to be weighed against the reasonably anticipated harm to civilians.[138]

Similar to the distinction principle, much of the proportionality assessment relies on context. A computer's ability to accurately make a proportionality assessment will depend on the environment in which it is making that assessment. In complex environments where the battlefield is fluid, for the reasons that follow, it will be extremely difficult for a computer to make proportionality assessments. This may not necessarily be the case in more static environments with few civilians present.

To comply with aspects of this principle, AWS will need to be able to make an assessment of the number of civilians or civilian objects likely to be harmed incidentally as a result of an

[135] Combe, above n 111, at 43. Noting that this technology currently needs contact with the head, but it is hoped that one day brain activity could be read from a distance.
[136] See Joint Commentary, above n 89; and Donnelly, above n 88.
[137] Henckaerts and Doswald-Beck, above n 107, rule 14 at 46.
[138] Anderson, Reisner and Waxman, above n 107, at 402; Schmitt and Thurnher, above n 2, at 254; Combe, above n 111, at 46; and Boulanin, Bruun and Goussac, above n 78, at 6-7.

attack relative to any concrete military advantage anticipated. Programming proportionality into AWS, is, in some respects, a much more complex task than programming AWS to distinguish lawful targets. Proportionality is a complex test, that requires weighing and judgement against a constantly changing battlefield, and has no accepted formula.[139] Terms such as "excessive" and "military advantage or value" are very context dependent to the surrounding fluid battle plans.[140] The proportionality assessment contains a tremendous number of variables, both in task and environment, that would be extremely difficult (if not impossible) to foresee at the programming stage. AWS would need to be constantly updated with the surrounding operations and battle plans and programming can, therefore, quickly become out of date.[141] To enable this proportionality assessment in complex environments, the AWS would need a significant degree of machine learning. While some have argued it may be possible[142], others argue that translating the requirements of proportionality into an algorithmic form is a significant challenge, and may never be possible.[143] Adding to this complexity, is that the AWS will also need to show its compliance with this core principle during the weapon's review.

Some scholars and states have argued that this assessment should only be made by a human.[144] Yet, while compliance with proportionality will be difficult for machines, it is equally difficult for humans.[145] Further, technology already exists to assist with this assessment. Various states use tools to assist with the proportionality assessment.[146] The United States military, for example, uses the Collateral Damage Estimate Methodology system, which allows commanders to make a proportionality assessment taking into consideration factors such as the precision of the weapon, tactics being employed, types of structures involved, blast effect, likelihood of civilians being present and the likelihood of injury or death to those civilians.[147] Yet, as currently configured, this system requires certain levels of authority and human intervention is still required. Humans are effectively in-the-loop for this assessment as, while the system is based on objective data and scientific algorithms, human operators provide the context specific data to overcome the machine learning limitations. Combe has also noted that certain technology, such as facial recognition and even machines perceiving brain activity from a distance, may be able to assist with aspects of the proportionality assessment.[148] As

[139] Anderson, Reisner and Waxman, above n 107, at 403.
[140] Schmitt and Thurnher, above n 2, at 256.
[141] Solis, above n 108, at 540.
[142] Schmitt and Thurnher, above n 2, at 256-257.
[143] Boulanin and Verbruggen, above n 21, at 25; Wyatt, above n 19, at 8; Sharkey, above n 26, at 380; and Anja Dahlmann and Marcel Dickow "Preventative Regulation of Autonomous Weapon Systems" (March 2019) German Institute for International and Security Affairs <www.swp-berlin.org> at 11.
[144] Docherty, above n 4, at 19; Joint Commentary, above n 89, at 1-2; and Comments by Italy, above n 130, at 2.
[145] Combe, above n 111, at 46.
[146] Laurent Gisel "The principle of proportionality in the rules governing the conduct of hostilities under International Humanitarian Law" (report prepared by the ICRC and University Laval for the International Expert Meeting, 22-23 June 2016, Quebec) at 56.
[147] Solis, above n 108, at 540.
[148] Combe, above n 111, at 62.

technology develops, therefore, it may be possible for AWS to be programmed with pre-determined values surrounding collateral damage to ensure compliance with the principle of proportionality.

Where it is effectively impossible to avoid civilian causalities, AWS should not be used. Nevertheless, provided AWS are either used in the right environment, or if it one day becomes possible to programme them in an appropriate manner, then AWS' use is unlikely to be deemed illegal by the proportionality principle. Given this, the proportionality principle is unlikely to be a strong basis for a pre-emptive ban on the development or use of AWS.

(c) Precautions in attack

An attacker has a duty of care to take feasible precautions in attack to minimise the harm to civilians and to exercise "constant care… to spare civilian population, civilians and civilian objects."[149] This principle is codified in article 57 of Additional Protocol I and is widely considered to be customary international law.[150] This principle includes providing a warning prior to an attack if circumstances permit and doing everything feasible to verify that the objectives to be attacked are nether civilians nor civilian objects and are not subject to special protection but are military objects.[151]

To complete this assessment as accurately as humans (if there is no human in or on the loop), a fully autonomous AWS would be required to use all their tools, such as onboard or external sensors, to ensure it did everything "feasible" to verify its targets are nether civilians nor civilian objects.[152] In many situations, this assessment would need to be made in complex environments that could not be known in advance of programming. In complex environments, therefore, this assessment would need some level of sophisticated machine learning, which presents a significant challenge.

On the other hand, Anderson, Reisner and Waxman suggest that the precautions in attack assessment may have limited relevance for most AWS. This is because the precautions in attack considerations are made at a higher level of command, which is not where the AWS operate.[153] The commander, for example, will make this assessment when planning an operation or attack. Specific weapons within that attack, as the AWS would be, would not.

When making this assessment, a state or a commander in the field must assess what system will better be able to protect civilians and civilian objects without sacrificing military advantage and choose the means which provides the lower risk. In some environments, AWS may actually

[149] Additional Protocol I, above n 91, art 57(2).
[150] Henckaerts and Doswald-Beck, above n 107, rule 15 at 51.
[151] Boulanin, Bruun and Goussac, above n 78, at 6-7.
[152] Feasible steps mean those that are "practicable or practically possible" given the existing circumstances, Thurnher, above n 100, at 190.
[153] Anderson, Reisner and Waxman, above n 107, at 404-405.

be able to *better* protect civilians or civilian objects.[154] Deployment of AWS in many environments could, therefore, be done without contravening this principle.

Under the precautions in attack principle, AWS could only be used lawfully when they are the most appropriate option to protect civilians or civilian objects. On this basis, Schmitt and Thurnher argue that a prohibition on AWS may actually work contrary to what IHL is trying to achieve.[155] This is for two reasons. Firstly, if a weapon system other than the AWS would better protect civilians or civilian objects, then that system should be used. This core IHL principle, in effect, prevents AWS being used in inappropriate situations. Secondly, a prohibition would prevent the use of AWS, when those systems could *better* protect civilians and civilian objects. A prohibition, it is argued, would be contrary to what IHL is attempting to achieve.

As with the other core IHL principles, the debate on AWS complying with the precautions in attack principle is far from complete. Yet, for all three core principles, it is unlikely that AWS will be automatically unable to comply with them. This means these principles alone are unlikely to support or necessitate a pre-emptive prohibition on AWS.

B Implications of the existing IHL regime to AWS

IHL has, over a long period of time, developed a robust set of rules for ensuring that the development and use of weapons is legal. It is internationally agreed that this existing regime applies equally to AWS.[156]

The debate on AWS' compliance with IHL is unlikely to be resolved any time soon. While this has not been an exhaustive review of AWS' applicability to IHL, what this discussion shows is that at this stage it is unlikely that AWS will be automatically held to be contrary to the existing IHL regime. This does not, however, end the discussion. On the contrary, the international context shows that these weapons will very likely be developed and there will be significant challenges that AWS will pose for IHL; with weapon reviews being just one example. The next question therefore becomes what, if anything, can be done to mitigate these risks? The GGE's eleven guiding principles are an attempt to mitigate the risks, but do they go far enough or can another mechanism be used to mitigate risk? This is where this dissertation turns to next.

[154] Thurnher, above n 100, at 190.
[155] Schmitt and Thurnher, above n 2, at 262.
[156] 2019 GGE Report, above n 33, guiding principle (a) at 13.

V Implementing Change via the CCW

The GGE meetings, operating under the legal framework of the CCW, have so far produced eleven guiding principles seeking to mitigate the risks raised by AWS. While this has been a considerable achievement, these principles are not free from criticism. Many of the guiding principles simply repeat existing IHL principles or are pitched at such a high level that they could be interpreted in various, sometimes diametric, ways. There are also concerns over how these guidelines will be implemented, operationalised and enforced. This Part examines the CCW to see what this treaty can do to mitigate the risks raised by AWS. This could include potential hard law options (such as adding a new protocol to the CCW) or soft law options (such as the GGE's guiding principles). While the specific content of the GGE principles will be considered later in this dissertation, this section considers the various mechanisms that the CCW provides to address the risks raised by AWS.

A Legal Basis for Implementing Change via the CCW

The CCW is a particularly useful piece of international law as it allows the challenges created by AWS to be addressed via two separate legal pathways. Firstly, it allows a new protocol to be negotiated and added to the CCW; so-called hard law. Alternatively, if that approach fails, it provides the forum for parties to negotiate and enter into other mechanisms for addressing challenges; a so-called soft law option.

1 Adding a new protocol to the CCW – hard law

The most common solution given to address the challenges raised by AWS has been to add a new protocol to the CCW.[157] This, in effect, would simply amend the existing CCW treaty. The CCW was deliberately negotiated as a chapeau convention, which only contains general provisions, and annexed protocols. This means all prohibitions or restrictions on the development or use of particular weapons are negotiated and attached as protocols to the CCW.[158] Article 8 of the CCW provides that any high contracting party may propose an additional protocol to be added to the CCW, which can be agreed upon at a subsequent meeting of the CCW.[159] States are not, however, obligated to accept any such proposed protocol.

---

[157] Docherty, above n 4, at 42; Anderson, Reisner and Waxman, above n 107, at 407; Metodi Hadji-Janev and Kiril Hristovski "Beyond the Fog: Autonomous weapon systems in the context of the international law of armed conflicts (Symposium on Governance of Emerging Technologies: Law, Policy, and Ethics)" (2017) 57 Jurimetrics Journal of Law Science and Technology 325 at 336.

[158] "Convention on Certain Conventional Weapons (CCW)" (2020) United Nations Mine Action Service <www.unmas.org>.

[159] CCW, above n 8, art 8.

Adding a new protocol to the CCW is not a radical idea, and there is precent for it. The Protocol on Blinding Laser Weapons is often the first example that AWS critics[160] point to as a pathway for AWS to follow.[161] This protocol was unique as it represented the first time since 1868 that a weapon was prohibited before it was used on the battlefield.[162]

The critics' argument is that the CCW is the correct mechanism to implement a prohibition on AWS by simply adding a new protocol that, similar to blinding lasers, prohibits AWS' development, deployment and use, before they ever hit the battlefield. The problem, however, lies with the limited international desire to do so.

A fundamental distinction between blinding lasers and AWS comes down to their military utility. Blinding lasers essentially only have one function, to incapacitate soldiers; and they do this in a permanent and particularly egregious manner. For this reason, these weapons could be seen as causing unnecessary suffering, contrary to article 35(2) of Additional Protocol I (or its customary law companion). Yet, this is not necessarily the case for AWS. As Neil Renic notes, there is a certain "viscerality" to blinding weapons and permanent blindness, whereas AWS, as weapons, are unlikely to differ significantly from their human-operated counterparts.[163] Autonomous technology is also useful in peaceful and civilian settings, further distinguishing it from blinding lasers.

The international context is also very different for AWS compared to blinding laser weapons. While there was some hesitation prior to a new protocol being generally accepted, when blinding laser weapons were close to becoming a reality, there was widespread support for their prohibition.[164] Ultimately, the protocol was accepted by a consensus of 44 states, including support from the United Kingdom and United States.[165] It is clear that, at this stage, there is not the same level of widespread support for prohibiting AWS. Given AWS also have the ability to revolutionise warfare and can potentially increase compliance with IHL, this is unlikely to change any time soon.

Without widespread support, it is unclear whether there would be sufficient support to even add a new protocol to the CCW or, even if there was, there would be limited value in doing so. Amendments to bilateral treaties can be straight forward, whereas this is often not the case with multilateral agreements. Article 8 of the CCW provides that high contracting parties may

---

[160] Docherty, above n 4, at 42; and Panama submission to the GGE as cited in Chairperson's Summary, above n 22, at 67.
[161] Additional Protocol to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects (Protocol IV, entitled Protocol on Blinding Laser Weapons) 1380 UNTS 370 (opened for signature 10 April 1981, entered into force 30 July 1998) art 1.
[162] Louise Doswald-Beck "New Protocol on Blinding Laser Weapons" (30 June 1996) 312 International Review of the Red Cross 272.
[163] Neil C Renic "Autonomous Weapon Systems: When is the time to regulate?" (26 September 2019) International Committee of the Red Cross <www.icrc.org>.
[164] Renic, above n 163.
[165] Doswald-Beck, above n 162.

propose additional protocols relating to other categories of conventional weapons not covered by the existing annexed protocols, which can be agreed by the high contracting parties.[166] As noted by article 40 of the Vienna Convention on the Law of Treaties (**VCLT**)[167], however, such amendment would be unlikely to bind the party to the original agreement that has not become a party to the amending agreement.[168] Applying that here, various states have already stated they are strongly opposed to any work aimed at a new treaty or similar measures, such as a new protocol to the CCW. This means it is unlikely in the near future that this particular hard law pathway will be successful.

2 Finding a soft law solution via the CCW – Soft Law

If agreement cannot be reached via hard law, the CCW also provides a forum to negotiate other soft law mechanisms. Unlike hard law, soft law is a concept that is not so easily defined. Soft law can be defined as international instruments that are not legally binding stricto jure[169] or, more simply, things that fall short of international law are called soft law.[170] This can include a variety of non-binding instruments such as codes of conduct, guidelines or statements of intent.[171]

Soft law can be particularly useful as a guide to interpreting hard law. A set of non-binding guidelines, for example, could have "legal effect" by shaping states' understanding of what constitutes compliant or acceptable behaviour with an underlying binding rule. Soft law could be seen as including non-binding rules or instruments that interpret or inform our understanding of binding legal rules or represent promises that in turn create expectations about future conduct.[172] Common examples of soft law instruments are the San Remo Manual on International Law Applicable to Armed Conflicts at Sea, the Tallinn Manual on the International Law Applicable to Cyber Warfare and the Manual on International Law Applicable to Air and Missile Warfare.[173]

---

[166] CCW, above n 8, art 8(2)(a)-(b).
[167] Vienna Convention on the Law of Treaties 1155 UNTS 331 (opened for signature 23 May 1969, entered into force 27 January 1980) [VCLT].
[168] Provided that original agreement does not provide otherwise, Alberto Costi, Scott Davidson and Lisa Yarwood "The Creation of International Law" in Alberto Costi (ed) *Public International Law: A New Zealand Perspective* (LexisNexis, Wellington, 2020) at 214. Here, the CCW does not.
[169] Costi, Davidson and Yarwood, above n 168, at 185.
[170] Andrew Guzman and Timothy Meyer "International Soft Law" (Spring 2010) 2 Journal of Legal Analysis 171 at 172.
[171] Costi, Davidson and Yarwood, above n 168, at 186.
[172] At 175.
[173] Michael N Schmitt (ed) *Tallinn Manual on the International Law Applicable to Cyber Warfare: prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge University Press, Cambridge, 2013); Louise Doswald-Beck *San Remo Manual on International Law Applicable to Armed Conflicts at Sea* (Cambridge University Press, Cambridge, 1995); and Harvard University Humanitarian Policy and Conflict Research *Manual on International Law Applicable to Air and Missile Warfare* (Cambridge University Press, Cambridge, 2013).

Soft law is not without its critics. Jan Klabbers, for example, decries it as a redundant concept that results in detrimental outcomes.[174] As it is inherently non-binding, there is also a risk that states will simply not comply with it and it has no real or effective means of enforcement. These are valid concerns, yet, there are a variety of reasons why states may nonetheless elect to enter into soft law. This can include, where there is relatively unambiguous existing hard law, the bureaucratic transaction costs of creating soft law instead of hard law can be lower.[175]

In the context of AWS, the GGE principles, a form of soft law, have already been agreed to by consensus at the GGE meetings. This is despite the above criticisms of soft law. Anderson, Reisner and Waxman have noted that soft law is only likely to get traction with states over time if it "largely codifies standards, practices, protocols and interpretations that states have converged upon over a period of actual development of systems."[176] This is perhaps why the GGE principles agreed to date, have either been replications of IHL or been pitched at a very high level, lacking much of the more radical detail that the critics demand.

As it will be the countries that do not want to enter into hard law mechanisms that will likely be the first to produce AWS, it is, in the author's opinion, critical to include them in any such mechanisms now. Fortunately, these states have already been participating in the production of the GGE's guiding principles.

B GGE's Guiding Principles

Over the past several GGE meetings, parties to the CCW have worked on creating a set of guiding principles in relation to AWS. As with many international negotiations, these principles were thoroughly discussed and subject to various last-minute amendments. Many proposed principles were discussed, but ultimately not agreed to. It is intended at future GGE meetings to add to these agreed principles.[177] The current set of eleven principles were agreed by consensus at the GGE, before being accepted (again by consensus) by the high contracting parties of the CCW.

The content of the GGE's principles is examined in detail below, however, at a high level, encompass a wide variety of matters associated with AWS. While there are various ways of categorising the GGE guiding principles[178], the principles can be ordered into four broad

---

[174] Jan Klabbers "The undesirability of soft law" (January 1998) 67 Nordic Journal of International Law 381 at 382-383.
[175] Guzman and Meyer, above n 170, at 177.
[176] Anderson, Reisner and Waxman, above n 107, at 407.
[177] Letter from Marc Pecsteen (Ambassador of Belgium and Chair of the GGE) to the high contracting parties of the CCW regarding a request for recommendations at the 2021 GGE meetings (26 April 2021) at 2.
[178] For example, the principles could be ordered along the life-cycle of the AWS, see Esther Chavannes, Klaudia Klonowska and Tim Sweijs "Governing Autonomous Weapon Systems" (17 March 2020) The Hague Centre for Strategic Studies <www.hcss.nl> at 28.

categories of risk that the principles are seeking to mitigate (noting there is a degree of overlap). This is shown in the following table 2.

Table 2:

Risks	What the GGE guiding principles seek to accomplish
1. What legal framework, if any, AWS fall under.	These principles consider the framework that AWS should operate under: guiding principles (a), (k).
2. The wider risks of developing, deploying and using AWS.	These principles address the wider risks resulting from the creation of AWS. This could include issues such as the proliferation of AWS and potentially lowering the threshold for war: guiding principles (f), (i), (j).
3. The risks associated with *developing* AWS.	These principles address the risks around developing AWS and whether certain guidelines could assist to ensure compliance with IHL: guiding principles (b), (d), (e), (g).
4. The risks associated with *using* AWS.	These principles address the risks around using AWS and whether certain guidelines could assist to ensure compliance with IHL: guiding principles (c), (h), (b), (d).

C Implementing, Operationalising and Enforcing the GGE Guiding Principles

The creation of the guiding principles at the GGE meetings is an important step forward to address the challenges created by AWS. Of significant concern, however, is exactly what role these principles should play and how they should be implemented and operationalised. Further, as it is a soft law mechanism, responsibility to comply with the guiding principles will fall to the individual states, with no real means of enforcement.

Such are these concerns, that this issue became an additional topic at the 2020 GGE meetings.[179] The GGE received 19 papers from states and organisations, including from the United States, ICRC, Campaign to Stop Killer Robots and a joint paper of which New Zealand was a contributor.[180] The GGE received a spectrum of responses on what role the principles should take, from creating common understandings[181] and providing guidance on existing IHL[182], through to being a foundation for negotiating a new treaty prohibiting AWS.[183]

Proposals for implementing the guiding principles were equally wide ranging, from statements that domestic laws should, and already do, encompass the guiding principles[184], establishing a

[179] "Draft Agenda" (draft agenda for the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, September 2020).
[180] Chairperson's Summary, above n 22, appendix III.
[181] Chairperson's Summary, above n 22, at 34 and 36.
[182] At 14 and 70.
[183] At 103.
[184] Russia 2021 Working Paper, above n 2, at 2-3.

compendium of best practice[185], through to suggestions of establishing a new operational framework.[186]

Critically, despite various useful suggestions and proposals, there does not appear to be a general consensus of the appropriate next steps to operationalise or implement these principles. Nor, therefore, is there any consensus for either compliance or enforcing this soft law mechanism. Unfortunately, the Covid-19 pandemic has further stifled progress on implementation, operationalisation and enforcement. The second session of the 2020 GGE meetings and the first session of the 2021 GGE meetings were cancelled due to the pandemic. It is hoped the GGE meetings scheduled for late 2021 will be able to proceed to further examine this issue.

This lack of agreement has not helped to quell the concerns of the critics. As noted above, there have already been calls that the guiding principles have merely served to perpetually avoid the key issues.[187] This begs the question, are there any mechanisms outside of the CCW that could be used to mitigate AWS' risks?

VI Implementing Change via Mechanisms Outside the CCW

Adding a new protocol to the CCW or implementing the GGE's guiding principles may have their challenges. Yet, the CCW is not the only legal avenue to address AWS' risks. There is nothing stopping the non-objecting states from simply negotiating and entering into an entirely new treaty prohibiting AWS, similar to the Treaty on the Prohibition of Nuclear Weapons (**TPNW**).[188] This Part examines these options, including how likely they are to be successful. It also draws on examples of other weapon systems, to see if a similar model could be adapted for AWS.

A Implementing Change Outside the CCW via Hard Law

Weapons treaties outside the CCW are nothing new to IHL. Over the past 50 years, there have been various treaties prohibiting or regulating various weapon technologies. This Part examines several of these to see if a similar approach could be taken with AWS.

1 Convention on Cluster Munitions and Convention on Anti-Personnel Mines

[185] "UK Commentary on the Operationalisation of the LAWS Guiding Principles" (Paper submitted to the Group of Governmental Experts, Geneva, 2020).
[186] Joint Commentary, above n 89.
[187] Moyes, above n 82; and Klijn and Okano-Heijmans, above n 26, at 9.
[188] Treaty on the Prohibition of Nuclear Weapons (opened for signature 20 September 2017, entered into force 22 January 2021).

Widespread consensus for a new CCW protocol prohibiting AWS is, in the author's opinion, unlikely to occur any time soon. Yet, prior to their signing, the Convention on Cluster Munitions[189] and the Convention on Anti-Personnel Mines[190] also did not have significant international support. These prohibitions were implemented by way of treaties (hard law), but their negotiation and signing followed a very different pathway to the implementation of the Protocol on Blinding Laser Weapons.

The Convention on Cluster Munitions has been signed by 108 parties, but notably it has not been signed by several powerful states, including the United States, China and Russia.[191] Similarly, the Convention on Anti-Personnel Mines has been signed by 133 states, but also not been signed by the United States, China, Russia and India.[192] This begs the obvious question, what profound change can these treaties purport to signal if the largest and most powerful states stand aside from them?[193]

It is argued that these treaties, even if not universally agreed with, create a stigma against particular behaviour (in this case, a stigma against the development and use of cluster munitions and anti-personnel mines).[194] On its face, such approaches could be applicable to AWS. As argued by Neil Renic, regulation, even without the support of the United States or Russia, would go a long way toward stigmatising the use of lethal autonomy in war.[195]

Yet, there are a number of key distinctions of AWS to cluster munitions and anti-personnel mines. Firstly, there is limited international support for a treaty prohibiting or strictly regulating AWS. At a state level, there are currently only around 30 states supporting such a ban.[196]

A further notable distinction is the military necessity associated with the weapons that these conventions prohibit. While both cluster munitions and anti-personnel mines are claimed to have military necessity,[197] they are not likely to have the influence over war that AWS may have. This is illustrated by President Putin's recent statements on AWS.[198] The investment in time and money that states are pouring into the technology underlying AWS, further illustrates the lengths that states are prepared to go to create these weapons.

---

[189] Convention on Cluster Munitions 2688 UNTS 39 (opened for signature 3 December 2008, entered into force 1 August 2010).
[190] Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and their Destruction 2056 UNTS 211 (opened for signature 3 December 1997, entered into force 1 March 1999).
[191] "6. Convention on Cluster Munitions" (27 December 2020) United Nations <www.treaties.un.org>.
[192] "5. Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction" (27 December 2020) United Nations <www.treaties.un.org>.
[193] Kenneth Anderson "The Ottawa Convention Banning Landmines, the Role of International Non-governmental Organisations and the Idea of International Civil Society" (2000) 11 EJIL 91 at 94.
[194] Erin Hunt "Stigmatizing Cluster Munitions: A Decade of Success" (October 2020) Arms Control Association <www.armscontrol.org> and Karen Hulme "The 2008 Cluster Munitions Convention: Stepping Outside the CCW Framework (Again)" (2009) 58 ICLQ 219 at 226-227.
[195] Renic, above n 163.
[196] Country Positions, above n 42.
[197] For example, the United States, China, Russia and India invoked military necessity as the reason for declining to sign the Convention of Anti-Personnel Mines. Lewis, above n 52, at 1317.
[198] President of Russia, above n 58.

Of further critical distinction, is the argument that AWS, unlike anti-personnel mines or cluster munitions, have the potential ability to one day *improve* compliance with IHL. Even today, autonomy is assisting to make weapon systems better able to comply with IHL. In Libya, for example, NATO commanders made an appeal to the United States for surveillance drones as these systems (or rather the autonomy within these systems) could loiter in the air for longer and therefore speed up the targeting process when the opportunity arose. The NATO-manned aircraft were reportedly too slow and had little loiter time to accurately target highly mobile vehicles before these targets surrounded themselves with civilians.[199]

The stigma against AWS is also reduced by the various commercial applications of AI. The Queensland University of Technology, for example, designed a robot to autonomously hunt and kill the invasive Crown of Thorns starfish, which is threatening the Great Barrier Reef.[200] As more of this technology is introduced into everyday life, like self-driving cars, the less weight this stigmatisation argument is likely to carry.

These are substantial distinctions and the argument that these conventions provide a roadmap for AWS is, in the author's opinion, significantly strained.

Even a prohibition in the model of cluster munitions or anti-personnel mines would not be fool proof. It is very difficult to accurately characterise and define AWS and current understandings and interpretations of AWS may never actually eventuate in practice. In this context, it is easy for particular interpretations to circumvent such a prohibition. We have already seen this in practice with the Convention on Anti-Personnel Mines. To continue joint operations with the United States, all of Canada, Great Britain and Australia interpreted various provisions of the Convention on Anti-Personnel Mines narrowly so as to not prohibit certain activity.[201] Similarly, the United Kingdom has claimed that, via its definition, AWS do not and may never exist.[202] Yet, under other definitions, AWS not only exist already, but have been actively used on the battlefield for years. It is not difficult to envisage how similar interpretations could be taken with a prohibition on AWS, particularly given our current understanding of this technology.

While these two existing conventions are useful case studies, the context for AWS is significantly different. So much so that, in the author's opinion, they cannot be used as realistic pathways for AWS.

---

[199] Anderson and Waxman, above n 118, at 1103.
[200] "New robot has crown-of-thorns starfish in its sights" (2 September 2015) Queensland University of Technology <www.qut.edu.au>.
[201] Christopher W Jacobs "Taking the next step: an analysis of the effects of the Ottawa Convention may have on the interoperability of the United States Forces with the Armed Forces of Australia, Great Britain and Canada" (2004) 180 MIL L Rev 49 at 113.
[202] UK Statement to IME, above n 16.

2 *Treaty on the Prohibition of Nuclear Weapons*

One of the fundamental differences between AWS and cluster munitions or anti-personal mines, is the military necessity obtained from these weapons. The same cannot be said for nuclear weapons. As noted at the start of this dissertation, nuclear weapons are considered the second revolution of warfare.

The TPNW was negotiated without sixty-nine nations, being all the nuclear weapon states and NATO members (aside from the Netherlands).[203] Notably, therefore, the United States, United Kingdom, Russia, China, France and various others have not entered into this treaty.[204]

The influence and military necessity that nuclear weapons carry highlights why states that have this capability are not prepared to give it up.[205] Similarly, states are very aware of the advantages that AWS will carry once they are developed, which is why they are spending the time and money that they are to develop them as quickly as possible.

As noted above, senior United States military leaders have already acknowledged that they may be compelled to develop AWS if their adversaries do.[206] While China has stated that the *use* of AWS should be prohibited, it does not think their development should be. Any treaty without the countries at the forefront of developing these weapons would therefore have limited ability to prevent or offset the risks or the harms that the treaty is seeking to prevent. John Williams has argued that the major players should be involved, stating "the UK and US should be prominent in this", when referring to a long-term regulatory framework.[207]

The TPNW also shows the weakness of the stigmatisation argument. Despite the apparent "stigmatisation" created by the TPNW, states with nuclear capability appear no closer to giving these capabilities up.[208]

Even were a treaty to be negotiated, Anderson and Waxman have warned that creating hard law at this stage, where the technology has not yet been developed, will inevitably favour categorical pronouncements and sweeping generalities and abstractions.[209] Indeed, similar issues have been seen with the TPNW. In the author's opinion, therefore, a treaty prohibiting AWS, as similar to the TPNW, would have limited value as the states that would not be subject to it are likely to be the ones develop this technology. Similar to cluster munitions and anti-

---

[203] Kevin Riordan "The Law of Armed Conflict" in Costi, above n 168, at 964.
[204] "Treaty on the Prohibition of Nuclear Weapons" (11 December 2020) United Nations <www.treaties.un.org>.
[205] See Ben Paxton "2017 saw 122 countries – but none of the nuclear weapon states – support the treaty for the prohibition of nuclear weapons. Why is nuclear disarmament so difficult and what should be the next steps for those aiming for prohibition?" (2019) 35 Medicine, Conflict and Survival 336 at 336-341.
[206] Sayler, above n 66.
[207] John Williams "Democracy and Regulating Autonomous Weapons: Biting the Bullet while Missing the Point?" (2015) 6 Global Policy 179 at 187. See also Lewis, above n 52, at 1318.
[208] Hans Kristensen and Matt Korda "The Treaty on the Prohibition of Nuclear Weapons Enters Into Force Today" (22 January 2021) Federation of American Scientists <www.fas.org>.
[209] Anderson and Waxman, above n 118, at 1112.

personal mines, therefore, while the TPNW is a useful comparator, it is unlikely to be a realistic pathway for AWS.

B Implementing Change Outside of the CCW via Customary International Law

A further possibility for addressing AWS' challenges, is via customary international law, which is defined as "evidence of a general practice accepted as law."[210] This law requires two elements, the objective practice of states and the subjective belief that this practice is rendered obligatory by the existence of a rule of law requiring it (opinio juris sive necessitatis).[211]

As shown in Part IV, there are various customary norms that apply fully to AWS. Yet, there is no customary law or norm that prohibits "autonomy" itself. Provided AWS can fit within IHL's principles, they are lawful. In fact, many modern weapons currently used on the battlefield which closely resemble AWS or have various elements of autonomy (such as the SeaRAM, Harpy or SGR-A1[212]) are not prohibited as being contrary to the core principles of IHL.[213]

Treaty law or a treaty norm, can, however, in certain circumstances, generate customary international law.[214] As noted in the North Sea Continental Shelf cases, a treaty norm may pass into the general corpus of customary international law as a result of the post treaty practice of states, so becoming binding even to states that have never become parties to that convention.[215] Indeed, article 38 of the VCLT provides that "Nothing in articles 34 to 37 precludes a rule set forth in a treaty from becoming binding upon a third State as a customary rule of international law, recognized as such."[216]

Powerful nations in particular can play a significant role generating customary norms.[217] Special weight is also given to those states specifically affected by the subject matter of the rule.[218] Helfer and Wuerth illustrate this with an example in the law of the sea, when the United States claimed jurisdiction and control over its continental shelf beyond its territorial sea. The speed at which the custom crystallised was described as 'striking', with President Truman's proclamation in 1945 and the norm being considered passe by 1958.[219]

---

[210] Yoram Dinstein *War Aggression and Self-Defence* (6th ed, Cambridge, Cambridge University Press, 2017) at 98.
[211] At 99.
[212] Boulanin and Verbruggen, above n 21.
[213] Anderson and Waxman, above n 118, at 1102.
[214] Dinstein, above n 189, at 95.
[215] *North Sea Continental Shelf (Federal Republic of Germany v Denmark; Federal Republic of Germany v Netherlands)* [1969] ICJ Rep 3 at 41.
[216] VCLT, above n 167, art 38.
[217] Laurence R Helfer and Ingrid B Wuerth "Customary International Law: An Instrument Choice Perspective" (2016) 37 Michigan Journal of International Law 563 at 584.
[218] Costi, Davidson and Yarwood, above n 168, at 162.
[219] Helfer and Wuerth, above n 217, at 584-585.

Critics of AWS may argue that, if a treaty prohibiting AWS is negotiated and implemented, then even without the objecting states, over time these states may amend their behaviour in line with this treaty. This may one day then crystalise into customary international law prohibiting AWS. Hadji-Janev and Hristovski propose a variant of this approach, with a treaty requiring meaningful human control in all AWS, that they hope will eventually crystallise into customary international law.[220]

What is distinct from the continental shelf example, however, is that there are no powerful nations, per se, that are leading the charge to prohibit AWS. On the contrary, there are several powerful states, such as the United States and Russia, that are attempting to do the exact opposite. Further, even if states did negotiate a treaty prohibiting AWS (or implementing requirements such as meaningful human control) with a view to develop similar customary international law over time, there are three doctrines that buttress the universality required of customary international law. This includes the position of new states, assertions of new custom and persistent objectors.[221] While the first two may not be persuasive in the context of AWS, the persistent objector doctrine may be. This doctrine provides that a nation that regularly and vociferously opposes an emerging custom will, if the new custom eventually forms, not be bound by the rule in its relations with other states.[222] Indeed, we have seen this approach taken in the nuclear weapons space. In the AWS context, the current practice and unambiguous statements of many states, including the United States and Russia, would squarely bring this doctrine into play.

There is certainly nothing stopping states independently negotiating and implementing a treaty absent the powerful states. Yet, from the perspective of one day hoping to create customary international law from such a treaty, it would appear unlikely to succeed.

C Implementing Change Outside of the CCW via a Quasi-Legislative Regime

A further option to address AWS' risks outside the CCW is a quasi-legislative regime similar to that created by the United Nations Security Council's Resolution 1540.[223] Resolution 1540 was created to address the risks of non-state actors obtaining weapons of mass destruction ("**WMD**") and requires states to implement certain domestic legislation to establish controls over WMD and the means to create and deliver them.[224]

A similar mechanism for AWS is unlikely to gain any initial traction to prohibit the development of AWS, when considering the current international context and likelihood of

---

[220] Hadji-Janev and Hristovski, above n 157, 337.
[221] Helfer and Wuerth, above n 217, at 570.
[222] At 571.
[223] SC Res 1540 (2004).
[224] Peter Crail "Implementing UN Security Council Resolution 1540: A Risk-Based Approach" (2006) 13 Nonproliferation Review 355 at 355.

getting agreement to such a resolution. Yet, it is easy to envisage a similar resolution yielding similar proliferation protections for AWS. The problem, however, lies with Resolution 1540's ambitious nature, which has posed significant challenges to its widespread adherence. No state has fulfilled all of its 1540 obligations.[225] It is difficult to see an AWS application being any different. It may also be more difficult to replicate a similar resolution in an AWS context. Much of the technology underlying AWS has not yet been, or is still in the process of being, developed. This makes it very difficult to accurately capture such a resolution. Further complicating matters, unlike WMD, a lot of technology underlying AWS will have civilian uses, such as autonomous cars, further undermining its effectiveness. Once AWS technology is better understood, a similar resolution may be more successful, however, it is likely too soon to implement a similar mechanism for AWS.

VII A Pragmatic Solution for Addressing Autonomous Weapon Systems' Challenges

The international context surrounding AWS has created a predicament. For the foreseeable future, it is unlikely that several states will stop their efforts to develop AWS. While the existing IHL regime will continue to apply to these weapons, AWS will undoubtably raise risks.[226] The GGE guiding principles are both a recognition of this and an attempt to address it. Against this background, this dissertation now considers what the most realistic and pragmatic solution for addressing the challenges raised by AWS could be.

A Building on the GGE Guiding Principles

In the author's opinion, for the reasons set out above, a hard law solution that garners widespread acceptance is an unrealistic proposition. A hard law solution would undoubtably be more robust and could place bespoke restrictions or limitations on the development, use and transfer of AWS. It could also address both enforcement and compliance. Yet, as the international context has made clear, it is extremely unlikely that the states currently developing AWS would agree to such a hard law option. Other hard law options absent these states, would have limited value as the states developing the AWS will not be part of it.

Instead, in the author's opinion, the most appropriate and realistic way to both address the emerging challenges of AWS and to achieve buy-in from the states currently developing these weapons is to build on the GGE's existing set of soft law principles. Indeed, guiding principle

[225] At 356.
[226] While not always advocating that the risks are insurmountable, see discussion on AWS' ability to comply with targeting laws in Sharkey, above n 53; Trumbull, above n 117; Schmitt and Thurnher, above n 2; Anderson and Waxman, above n 118; Thurnher, above n 100; and Boulanin, Bruun and Goussac, above n 78.

(k), which was accepted by consensus at the GGE meetings, provides that the CCW is an appropriate mechanism to be discussing the challenges raised by AWS.[227]

This soft law approach has its weaknesses. It will almost certainly be less robust than a hard law approach, as it is inherently non-binding in nature. As such, there is nothing requiring states to comply with it, and no real means of effectively enforcing it. To date, states have been unable to agree on how to implement, operationalise and enforce these principles. It does not look like this will change any time soon.

Yet, something is still better than nothing. As noted by Lewis, a regulatory scheme that induces partial compliance is still more effective than a ban that induces none.[228] Despite soft law's weaknesses, states have already bought in to other soft law mechanisms, such as the San Remo Manual and the Tallinn Manual. Further, the GGE guiding principles have already been accepted by consensus, showing states are open to a soft law approach.

A soft law approach has further benefits too. It allows the continued participation of non-governmental stakeholders, such as SIPRI or the ICRC, which have made valuable contributions to the international debate.[229] Soft law also has the benefit of being less rigid than hard law options. While certain recommendations may not be palatable now, this is not to say they will not be in the future, once technology has further developed and is better understood.

The establishment by the GGE of its soft law guiding principles does not, however, mean that AWS' risks have been adequately managed. On the contrary, critics are quick to point out that they do not go far enough.[230] Many of the principles simply repeat existing IHL or are pitched at such a high level that it is hard to understand how states will comply with the principle in practice.

The GGE's guiding principles have created a solid foundation for addressing AWS' risks. This dissertation now examines the existing content of the GGE's guiding principles and considers whether any additional content can be added to mitigate the risks created by AWS. If additional content will assist, it will require a balance of providing as much detail as possible, while still garnering widespread acceptance.

B The Appropriate Legal Framework and the Wider Risks of Development

The first category of GGE principles examine what can be done to mitigate the wider risks associated with AWS' development. Rather than looking at bespoke IHL considerations, these guidelines seek to address more holistic issues such as impacts on regional stability. The GGE

[227] 2019 GGE Report, above n 33, guideline (k) at 13.
[228] Lewis, above n 52, at 1318.
[229] Klijn and Okano-Heijmans, above n 26, at 17.
[230] Chairperson's Summary, above n 22, at 39; Moyes, above n 82; and Klijn and Okano-Heijmans, above n 26, at 9.

meetings have so far agreed to five principles in this broad risk area (guiding principles (a), (f), (i), (j), (k)). This Part looks at these principles and considers whether any additional content could assist to mitigate risk.

1 The appropriate legal framework for AWS

There are two GGE guiding principles that address which legal regime AWS should be subject to. Firstly, principle (k) provides that the CCW is the appropriate mechanism and legal framework to address challenges raised by AWS.[231] Secondly, principle (a) provides that IHL continues to apply fully to all AWS, including their development and use.[232] These principles are not, in themselves, controversial.

Some scholars have suggested that these more holistic principles could go further to specifically address the role of humans in AWS. This could, for example, include requirements for "human responsibility", to ensure that any AWS attack complies with the laws of war.[233] In the author's view, arguments with human involvement are better addressed in the development and use of AWS, rather than more holistic risks that these principles seek to address. No additional content to the GGE's principles is proposed.

2 The wider risks of developing, deploying and using AWS

The GGE meetings have so far produced three principles addressing the wider risks associated with developing, deploying and using AWS. Yet, it is argued that these principles do not go far enough and more can be done to mitigate the wider risks created by AWS.[234]

(a) Proliferation of AWS

Concerns that the development, deployment and use of AWS will result in proliferation of AWS has been a concern of critics for some time.[235] Similar to nuclear weapons, there are concerns that AWS may fall, or be transferred into (directly or indirectly), the hands of terrorists, criminals or rogue states.[236] Indeed, this was the impetus for the United Nations Security Council's Resolution 1540. Without intervention, significant numbers of AWS may be developed and, as geopolitical pressures rise, states may be forced to employ AWS prior to

---

[231] 2019 GGE Report, above n 33, guideline (k) at 13.
[232] 2019 GGE Report, above n 33, guideline (a) at 13.
[233] Ronald Arkin and others "Autonomous Weapon Systems: A Roadmapping Exercise" (9 September 2019) Georgia Institute of Technology <www.cc.gatech.edu> at 6.
[234] Moyes, above n 82, at 3-4.
[235] Docherty, above n 4, at 29-30; and Sharkey, above 53, at 182.
[236] Docherty, above n 4, at 37.

the machines being ready. These significant concerns, it is argued, outweigh any potential benefits that may arise from AWS.[237]

Conversely, Anderson argues that it is actually easier and cheaper to use existing weapons to create mass destruction, than it is to source and use new or emerging technologies.[238] Similar arguments were made by the critics of drones, prior to their development and use. Yet, large scale military UAVs are rarely, if ever, found in the hands of non-state actors.[239]

The GGE meetings have addressed these concerns with guiding principle (f), which states that when developing or acquiring AWS, physical security, appropriate non-physical safeguards, the risk of acquisition by terrorist groups and the risk of proliferation should be considered.[240] While the intent here is clear, given these matters only need to be "considered", it is not clear how useful this guideline will be in practice.

There have been various solutions proposed to mitigate these risks. A collection of scholars from various institutions[241], produced a working paper titled "Autonomous Weapon Systems: A Roadmapping Exercise" (**Roadmapping Exercise**).[242] In this paper, the authors propose requiring specific measures to render weaponisable robots less harmful. This could be achieved via mechanisms such as geofencing or hard-wired kill switches.[243] Such bespoke measures would certainly assist to reduce the chance of these weapons being used by non-state actors. Yet, in the author's view, such specific limitations are unlikely to receive widespread acceptance at this stage, as they could be seen as inhibiting AWS' development.

An alternate approach to prevent proliferation could be limiting the transfer of AWS, either of AWS themselves or the components that comprise AWS. This would be similar to the effect of both Resolution 1540 and the unrelated Arms Trade Treaty ("**ATT**"), a regime that has proven very successful for conventional arms.[244] It is unlikely, given the language it uses (such as "combat aircraft" and "missiles"), that the scope of the ATT would currently encompass AWS. Limiting the transfer of AWS could be implemented via targeted multilateral controls to prevent large-scale sale and transfer of weaponisable robots and related military-specific components for illicit use.[245] Such a measure would likely need to occur via hard-law and would likely face similar opposition to other hard law proposals suggested in the AWS space.

---

[237] Daniele Amoroso and Guglielmo Tamburrini "In search of the 'Human Element': International Debates on Regulating Autonomous Weapon Systems" (2021) 56 The International Spectator 20 at 25.
[238] Anderson, above n 79, at 34.
[239] At 31.
[240] 2019 GGE Report, above n 33, guideline (f) at 13.
[241] Including the Georgia Institute of Technology, Massachusetts Institute of Technology, Berkeley, Stanford University, Cornell University and University of New South Wales.
[242] Arkin and others, above n 233.
[243] Arkin and others, above n 233, at 7.
[244] Arms Trade Treaty 52 ILM 988 (opened for signature 3 June 2013, entered into force 24 December 2014). See Pablo Olabuenaga "Why the Arms Trade Treaty Matters – and Why It Matters That the US Is Walking Away" (8 May 2019) Just Security <www.justsecurity.org>.
[245] Arkin and others, above n 233, at 7.

As noted by Klijn and Okano-Heijmans, the current geopolitical climate does not seem conducive to new multilateral arms control.[246]

Alternatively, states could develop an industry cooperation regime analogous to that mandated under the Chemical Weapons Convention. This regime requires that manufacturers know their customers and report suspicious purchases of significant quantities of items such as fixed-wing drones, quadcopters, and other weaponisable robots.[247]

The United States addresses proliferation in its Department of Defense directive, but reverts to its existing practices with a policy that provides: "International sales or transfers of autonomous and semi-autonomous weapon systems will be approved in accordance with existing technology security and foreign disclosure requirements and processes…"[248] The author is unaware of other states having specific AWS proliferation policies.

The potential for proliferation is an issue that links almost every weapon system and considerable experience can be gained from how other weapon systems have approached this issue. There is also little doubt that this experience will be used at some stage. Yet, any guideline that goes further than the high-level principle (f) would, in the author's opinion, be unlikely to achieve widespread acceptance at this stage. It is easy to see how states could lean on the fact that the development of large-scale military UAV drones did not result in widespread proliferation[249] to delay the imposition of any such measures that could inhibit AWS' development. Accordingly, this dissertation does not propose to add any content in addition to the agreed GGE principle (f).

(b) Addressing other broader risks with the development, deployment and use of AWS

In addition to proliferation, there have been a number of other broader concerns that states, organisations and scholars have raised with the development and use of AWS. These include that AWS will lower the threshold to go to war, will raise the propensity to go to war and may even encourage the start of a new arms race.[250]

The GGE meetings have so far produced two guiding principles to address such issues. Firstly, the GGE sought to address the risk that machines would be treated like humans (so called, anthropomorphising), which diminishes the role that humans play in war. Principle (i) is clear: "In crafting potential policy measures, emerging technologies in the area of lethal autonomous weapons systems should not be anthropomorphized."[251] Secondly, to address concerns that

[246] Klijn and Okano-Heijmans, above n 26, at 14.
[247] At 5.
[248] DoD Directive, above n 11, at 3.
[249] This relates primarily to large-scale military UAVs. Smaller drones, available over the counter for civilian use, are being used by non-state actors and terrorist organisations.
[250] Sharkey, above n 53, at 182; and Docherty, above n 4, at 29.
[251] 2019 GGE Report, above n 33, guideline (i) at 13.

innovative or beneficial uses of AWS may be inhibited, principle (j) provides: "Discussions and any potential policy measures taken within the context of the CCW should not hamper progress in or access to peaceful uses of intelligent autonomous technologies."[252]

Yet, critics suggest the two GGE principles do not go far enough.[253] The authors of the Roadmapping Exercise, for example, have proposed a requirement that, when developing AWS, a risk assessment must address the effects these weapons will have on "geopolitical destabilization, accidental escalation, increased instability due to uncertainty about the relative military balance of power, and lowering thresholds to initiating conflict and for violence within conflict".[254]

On its face, this proposal is pitched at a similar high level to above GGE principle (f). It attempts to balance risk, without tying states down to specifics. The problem, however, is that this guideline drifts into the realm of politics, a notoriously complex and fluid area. Requiring a specific assessment on issues such as "geopolitical destabilisation" prior to the development or deployment of AWS, is unlikely to garner widespread support, particularly with certain powerful states.

Yet, in the author's view, there is scope to add "accidental escalation" to the range of factors that should be "considered" when developing AWS. This consideration is similar to those factors already addressed in guiding principle (f). On a more literal interpretation, preventing accidental escalation may include preventing AWS from going rogue (akin to ensuring there are appropriate physical and non-physical safeguards). On a wider interpretation, accidental escalation touches on risks similar to proliferation. As with the other aspects of principle (f), a state would not be required to disclose these considerations to other states.

Rather than creating a bespoke principle, this concern could be added to the existing GGE principle (f), as set out in red in table 3.

Table 3:

Proposed additional content to the GGE guiding principles
a) When developing or acquiring autonomous weapon systems, physical security, appropriate non-physical safeguards, the risk of acquisition by terrorist groups, the risk of accidental escalation and the risk of proliferation should be considered.

[252] 2019 GGE Report, above n 33, guideline (j) at 13.
[253] Moyes, above n 82, at 3.
[254] Arkin and others, above n 233, at 8.

VIII Guidelines to Ensure Compliance with IHL during AWS' Development and Use

Placing the more holistic risks associated with AWS to one side, we now turn to whether any additional content can assist to ensure AWS' compliance with IHL during their development and use. These guidelines look at more specific issues such as whether weapons reviews could be adjusted to better capture this new and opaque technology. The GGE meetings have so far agreed six principles in this risk area (guiding principles (b), (c), (d), (e), (g), (h)).

A The Risks Associated with Developing AWS

Several of the GGE's guiding principles are directed at ensuring IHL compliance during the weapon's development. Yet, critics have suggested that more could be done during the weapon's development to best ensure it complies with IHL.[255] This Part examines whether any additional content could both assist with IHL compliance and be widely accepted.

1 Imposing a requirement for meaningful human control in the development of AWS

Perhaps the hottest topic in the AWS debate over the past several years is the role that humans should play in the development, deployment and operation of AWS. It is uncontroversial that human control, at some level, must be retained over AWS. This is consistent with statements made by a number of states and organisations, including the ICRC[256], Israel[257], the United States[258] and New Zealand.[259] Yet, exactly how this translates into the development of AWS, is not entirely clear.

The GGE meetings have so far produced one principle concerning human involvement and the "use" of AWS (examined in detail below). Effectively, however, this principle equates to a requirement that states comply with existing IHL. Not surprisingly, critics argue this principle does not go far enough and a requirement for "meaningful human control" must be imbedded during the *development* stage of AWS.[260]

The organisation Article 36, a staunch critic of AWS, has proposed regulating AWS by requiring they are developed with certain levels of human involvement in the AWS' process

---

[255] See Moyes, above n 82; and Sharkey, above n 53.
[256] "Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons" (15-16 March 2016) International Committee of the Red Cross <www.icrc.org> at 83.
[257] "Israel Considerations on the Operationalisation of the Eleven Guiding Principles Adopted by the Group of Governmental Experts" (Paper submitted to the Group of Governmental Experts, Geneva, 31 August 2020) at 3.
[258] Heather Roff "The Ontology of Autonomy for Autonomous Weapon systems" (Podcast, 5 April 2017) University of Oxford <www.podcasts.ox.ac.uk>; Wareham, above n 52; and Boulanin and Verbruggen, above n 21, at 64.
[259] Ballard, above n 84.
[260] Moyes, above n 39; Moyes, above n 82, at 2; and Sharkey, above n 53, at 184.

functioning. Process functioning means the processes from sensor collection, calculation and implementation of force.[261] Another approach involves regulating the "human machine team". The human machine team determines how work is allocated within teams of humans and automated agents.[262] The goal of this second approach is to ensure compliance with IHL, but not necessarily to prescribe where a human operator should be within a team. This has the advantage of avoiding specific granular debates that have bogged down this issue to date. A further, more holistic approach, could see AWS being regulated so they can only be developed in accordance with a moral framework.[263]

A similar approach was put forward in a 2020 joint commentary submitted to the GGE by nine states, including New Zealand, which advocated establishing an operational framework with certain requirements of human control. This framework would require that AWS be developed so they are capable of understanding operational context and have situational awareness. Limits of human-machine interaction would also be imposed, ensuring there is "meaningful human control" in the machine's critical functions and imbedding requirements to prevent redefinition of missions without human intervention.[264]

As we have seen, however, existing IHL already contains elements of human involvement or control, without (arguably) the need to prescribe new restrictions during development. The precautions in attack principle, for example, requires a human to make the judgement of when to attack and with what weapon. Even with fully autonomous weapons, Anderson, Reisner and Waxman argue a human element will likely remain.[265] Humans, for example, will make the decision on when an AWS will be deployed and in what environment. While this human involvement is implemented during the *use* of the AWS, as opposed to the development, it demonstrates that human involvement is already imbedded in the overall IHL process and further guidelines may not be required, at a granular level, during the developmental stage.

Imposing requirements for meaningful human control also raises the criticism that implementing guidelines prior to the development of the technology, imposes abstract principles rather than concrete rules.[266] Creating limitations during development is also easier said than done. As noted by the United States Congressional Research Service, there is no one-size-fits-all level of human judgement and appropriate levels of human judgement over force

[261] Moyes, above n 39. Amoroso and Tamburrini propose a variant of this approach, with minimal human control requirements but there are exceptions for use of AWS in certain situations, above n 237, at 30-32.
[262] Karen M Feigh and Amy R Pritchett "Requirements for effective function allocation: A critical review" (2014) 8 J Cognitive Engineering and Decision Making 1, at 33-51, as cited in Marc Cannellos and Rachel Haga "Lost in Translation: Building a Common Language for Regulating Autonomous Weapons" (9 September 2016) 35 IEEE Technology and Society Magazine 50 at 54; and Combe, above n 111, at 63-64.
[263] Bellis, Torres and Umbrello, above n 80, at 278. Although, ultimately, the authors acknowledge the practical difficulty of adopting such a framework.
[264] Joint Commentary, above n 89.
[265] Anderson, Reisner and Waxman, above n 107, at 403-404.
[266] Anderson, above n 79, at 39.

can differ across weapon systems, domains of warfare, types of warfare, operational contexts and even across functions in a weapon system.[267]

Existing attempts by critics to formulate limits of human control in weapon systems have already resulted in conflicting and confusing accounts.[268] Cannellos and Haga compared two definitions of meaningful human control proposed by the organisations Article 36 and ICRAC, and found it was entirely unclear what types of human control they agreed and disagreed on.[269] The definitions used by these organisations would likely result in some weapons, that are currently being used on the battlefield today, being considered illegal under IHL when those weapons are otherwise widely considered lawful.[270]

Until AWS technology is further developed and better understood, it is difficult to see certain states agreeing to limitations or obligations. The human machine team proposal, that seeks compliance with IHL rather than imposing certain prescribed limits, is the most likely to receive widespread acceptance. Yet, in the author's view, even this mechanism could be seen to stifle development. Even were this not the case, accurately capturing such a bespoke limitation is an extremely difficult task, as illustrated by the existing attempts to do so. As compliance with soft law is reliant on individual states, imposing limits of human control into the development of AWS risks states disengaging with the principles in their entirety. Nor does parking these requirements, for now, necessarily mean such limitations cannot be returned to at a later date, when the implications of such limitations are better understood. While these restrictions would assist with IHL compliance, at this stage, the author considers any additional content to the GGE principles imposing certain levels of meaningful human control will be very unlikely to be widely accepted.

2 Ensuring accountability during the development of AWS

A related argument to requiring meaningful human control over AWS, is ensuring that human accountability is retained. That is, ensuring that accountability is not transferred to machines. The GGE meetings have so far agreed two principles that address accountability. GGE principle (b) provides: "Human responsibility for decisions on the use of weapons systems must be retained since accountability cannot be transferred to machines", while principle (d) provides:[271]

> Accountability for developing, deploying and using any emerging weapons system in the framework of the CCW must be ensured in accordance with applicable international law,

[267] Sayler, above n 66.
[268] Cannellos and Haga, above n 262, at 52.
[269] At 52.
[270] At 53.
[271] 2019 GGE Report, above n 33, guidelines (b) and (d) at 13.

> including through the operation of such systems within a responsible chain of human command and control.

The United States, in its directive, attempts to provide some more specificity with regards to human control and accountability. A United States policy provides: "Autonomous and semi-autonomous weapon systems shall be designed to allow commanders and operators to exercise appropriate levels of human judgement over the use of force".[272] A second policy provides:[273]

> Semi-autonomous weapon systems that are onboard or integrated with unmanned platforms must be designed such that, in the event of degraded or lost communications, the system does not autonomously select and engage individual targets or specific target groups that have not been previously selected by an authorized human operator.

While there are no specific levels or limits, both of these policies ensure the weapon is designed so that human control is retained during that weapon system's use. While not referred to specifically, presumably this human operator would then become liable should there be a breach of IHL.

The United States' policies are consistent with statements made by a number of states and organisations that human control, at some level, must be retained over AWS, as noted above. This is also consistent with proposals from the Canberra Working Group[274], which provide AWS should be designed so they can be operated pursuant to a commander's intent and should be implemented into militaries in a way that is coherent with command and control.[275]

The author considers it unlikely that states will go further than these higher level statements and require new specific thresholds of meaningful human control to be imbedded into AWS during their development. Yet, higher level, context specific guidelines add clarity to the accountability concerns and strike an appropriate balance between addressing human control and accountability, while encouraging widespread buy-in. In the author's view, it would be appropriate to add the substance of these policies to the existing GGE principles, as set out in table 4.

Table 4:

Proposed additional content to the GGE guiding principles
a) Autonomous weapon systems shall be designed to allow commanders and operators to exercise appropriate levels of human judgement over the use of force.

[272] DoD Directive, above n 11, at 2.
[273] DoD Directive, above n 11, at 3.
[274] The Canberra Working Group is an international group of scholars who met in April 2019 to discuss the practical, legal, ethical and operational considerations presented by AWS.
[275] Deane-Peter Baker and others "Guiding Principles for the Development and Use of LAWS Version 1.0" (April 2019) E-International Relations <www.e-ir.info> at 3-4.

b) Autonomous weapon systems shall be designed such that, in the event of degraded or lost communications, the system does not autonomously select and engage individual targets or specific target groups that have not been previously selected by an authorised human operator.

3 Development of AWS and weapon reviews

When developing or acquiring new technology, there is a duty on all states to consider whether the use of a new weapon or technology (including AWS) would, in some or all circumstances, breach the international rules that apply to that state (see Part IV). Article 84 of Additional Protocol I (for those subject states) arguably requires states to share its review procedures. Yet, as acknowledged by Lawland, article 36 of Additional Protocol I does not state how a weapon review is to take place and each state has the discretion of whether to allow access to those review records, in whole or in part, and to whom.[276]

A risk raised by many states, organisations and scholars is that, as the algorithms that sit behind AWS become more complex, it will be harder to comply with this existing IHL rule.[277] This issue is perhaps best illustrated by the black box problem. This is where the inputs and outputs of an AWS are observable, but the actual process from input to outcome is unknown or becomes a "black box."[278]

The GGE meetings have so far agreed to guiding principle (e), a replication of the existing IHL weapons review laws, as well as ensuring "risk assessments and mitigation measures" are part of the design, development, testing and deployment of AWS (principle (g)).[279]

In addition to principles (e) and (g), various proposals have been put forward to ensure AWS can best comply with weapon review laws. The ICRC, in its 2020 commentary on the GGE's guiding principles, proposed that, during weapon reviews, particular attention should be given to measures to ensure there is human control over weapons and the use of force.[280] As we have seen, however, putting such statements into practice has proven troublesome.

To ensure AWS technology is both fully understood in theory, as well as practice, Waxman and Anderson have suggested that weapon reviews will need to be formulated with collaboration between the private sector and governments, as well as military commanders, lawyers, weapon designers and engineers.[281] This is to ensure that the full range of risks raised by the AWS are fully understood across that weapon's entire life cycle, including any

[276] Lawland, above n 101, at 933 and 955.
[277] Docherty, above n 4, at 33-36; Sharkey, above n 53, at 180-181; and Boulanin, Bruun and Goussac, above n 78, at 28-30. Various states have emphasised the importance of weapons reviews in recent submissions to the GGE, see Chairperson's Summary, above n 22, at 4-5, 16 and 92.
[278] Boulanin and Verbruggen, above n 21, at 17.
[279] 2019 GGE Report, above n 33, guidelines (e) and (g) at 13.
[280] ICRC Commentary, above n 3, at 2.
[281] Anderson, Reisner and Waxman, above n 107, at 408-409; and Boulanin, Bruun and Goussac, above n 78, at 29.

deployment. Liaison with the private sector is also acknowledged by John Williams, who notes "it is the commercial sector that we must look for the delivery of future disruptive technology."[282] While involvement with the private sector recognises the reality of where this technology will likely come from, it also raises potential problems with secrecy and intellectual property theft. Militaries are not quick to give away their secrets and commentators have already acknowledged China's covert attempts to develop AWS technology via intellectual property theft and industrial espionage.[283] These concerns may mean that states will be reticent to involve private entities any more than they need to, if at all.

Given the complexity of the technology underlying AWS, there is little doubt that weapons reviews for AWS will need to occur at an earlier stage. This could include guidance at the design stage, with new forms of testing and verification being required.[284] It seems reasonable that a high level principle in this regard would be generally acceptable.

In terms of content, as acknowledged by Waxman, the existing weapon reviews will need tweaking to account for complex, software driven systems. This could occur by evaluating those systems with reliability engineering and against certain performance standards.[285] Any legal standards will need to translate into terms that are "testable, quantifiable, measurable and reasonable".[286] A weapons review will need to occur across the design, demonstration and manufacture of the AWS and consider in-service deployment.

The United States has an internal policy that stipulates autonomous systems will go through rigorous hardware and software verification and validation, and realistic system development and operational tests and evaluation. It also proposes establishing training, doctrine, tactics, techniques and procedures to ensure that system will function as anticipated in realistic operational environments against adaptive adversaries.[287]

While many of these proposals amount to restatements of existing IHL, they nonetheless do so in the specific context of AWS. They also address some of the risks raised by AWS' critics. In the author's view, a high level principle incorporating aspects of these proposals would be generally acceptable, provided it is pitched at a high level so as not to inhibit the development of AWS.

High level principles such as this, while being more likely to receive general acceptance, run the risk of being difficult to implement in practice. Yet, this is also the very nature of weapons reviews. As Lawland notes, each state has a significant amount of discretion over how it conducts its reviews and who it discloses it to.[288]

---

[282] Williams, above n 207, at 186.
[283] Piccone, above n 69.
[284] Anderson and Waxman, above n 118, at 1104 and 1113.
[285] Anderson, above n 79, at 21.
[286] Anderson and Waxman, above n 118, at 1104 and 1113.
[287] DoD Directive, above n 11, at 2.
[288] Lawland, above n 101, at 933 and 955.

The authors of the Roadmapping Exercise consider a further principle that would assist weapons reviews is designing control systems to require operator identity authentication and unalterable records of operation. This would enable post-hoc compliance checks in case of plausible evidence of non-compliant autonomous weapon attacks, assisting.[289] This would also seek to address the concerns that many critics have with understanding what an AWS has done, the so-called black box problem.

Given much of this technology has not yet been developed, requiring a specific mechanism such as an "operator identity authentication" for every AWS is unlikely to gain widespread agreement. Yet, in the author's view, requiring unalterable records of operation may and this would greatly assist with the weapons review process. Such a guideline would not require a specific record to be kept (such as a line of specific coding), but would rather require *a* record of operation to be kept that could not be changed after the fact. As with every soft law principle, an individual state would need to be relied on to implement and comply with this, but critically it would be the one controlling those records and would not be required to disclose them. This appears to strike the necessary balance of addressing risk, but not inhibiting development. The author therefore considers the following content could be added to the GGE's guiding principles, as set out in table 5:

Table 5:

Proposed additional content to the GGE guiding principles
a) When developing autonomous weapon systems, weapons reviews should occur at an early stage to ensure compliance with international law. b) Autonomous weapon systems should go through rigorous hardware and software verification and validation and realistic system development and operational tests and evaluation. c) Training, doctrine, tactics, techniques or procedures should be established to ensure autonomous weapon systems function as anticipated in realistic operational environments against adaptive adversaries. d) Autonomous weapon systems should be designed with an unalterable record of operation.

4 Development of AWS and compliance with targeting laws

Part IV of this dissertation finds that AWS are unlikely to be illegal per se. IHL still requires, however, that the use of any AWS will need to comply with the assessments of distinction, proportionality and precautions in attack (amongst other IHL principles). These assessments will need to be incorporated into the development of AWS, to the extent possible, or left to humans to make.

The GGE meetings have so far produced one guiding principle that touches on AWS' development at a high level. Principle (f) provides that when developing new weapons systems,

[289] Arkin and others, above n 233, at 5.

physical security and appropriate non-physical safeguards (including cybersecurity against hacking or data spoofing) should be considered.[290]

Scholars have proposed various solutions during the development stage that go further than principle (f), to ensure that AWS comply with IHL. This could be achieved via prohibitions on certain weapon designs. For example, a prohibition on designs that allow a machine to be converted from a compliant system (or a compliant mission) to non-compliant one via software updates.[291]

Alternatively, instead of prohibiting certain designs, there could be certain requirements that AWS *must have* in their design. These requirements could regulate that system's ability to identify, select and engage a target. This could be achieved with a requirement that AWS only be allowed to "see" and engage certain targets (such as targets with certain emissions).[292] Deployment could be restricted to only those AWS that meet certain sensory standards (such as computational ability or onboard camera capabilities[293]) so that system could make reasonably foreseeable distinction-based decisions on the battlefield.[294] There could also be a requirement designed into AWS that it can only initiate an attack with human authorisation,[295] which could be achieved via "air-gapped firing authorisation circuits" that are connected to a remote human operator and not the on-board automated control system.[296]

There are other ways to regulate AWS' development too. AWS could be required to have explainable artificial intelligence[297] or be able to make assessments and learn from its encounters.[298] Bellis, Torres and Umbrello propose a requirement that AWS must have the capacity for judgement calls that are equal to or greater than humans.[299] Taking a slightly different approach, Chavannes and others have proposed an internationally agreed "Ethical Governor" algorithm check, which vets whether an AWS' decision accords with IHL and, if so, responds to its particular operational orders (although they acknowledge such an algorithm does not yet exist).[300]

These suggestions will almost certainly assist with AWS' compliance with IHL, yet there is perhaps one other thing that connects them all. They all propose certain requirements or limitations into AWS' design. GGE principle (f), on the other hand, is pitched at a higher level, with physical safety and non-physical safeguards being considerations rather than specific

[290] 2019 GGE Report, above n 33, guideline (f) at 13.
[291] The Roadmapping Exercise notes that proofs can, in principle, be provided using cryptographic techniques that allow the proofs to be checked by a third party without revealing any details of the underlying software. Arkin and others, above n 233, at 6.
[292] Combe, above n 111, at 46.
[293] Lewis, above n 52, at 1323.
[294] Anderson, Reisner and Waxman, above n 107, at 407.
[295] Arkin and others, above n 233, at 6.
[296] At 5.
[297] Chavannes, Klonowska and Sweijs, above n 178, at 24.
[298] Lewis, above n 52, at 1323.
[299] Bellis, Torres and Umbrello, above n 80, at 278.
[300] Chavannes, Klonowska and Sweijs, above n 178, at 25.

requirements. In the author's opinion, any measures inhibiting or preventing the development of AWS are unlikely to gain widespread acceptance. It seems extremely unlikely a state would limit itself, potentially to an adversary's advantage. One could also envisage arguments where, in certain situations, a characteristic that is required to be imbedded into an AWS actually makes that weapon unable to comply with IHL. As a soft law mechanism, it is likely states would simply ignore any such limitations. Problematically, however, this may encourage states to ignore other principles.

Nor, however, does this mean that AWS are likely to be developed carte blanche, with no further thought given to IHL and human control. On the contrary, the existing IHL regime will still regulate the development of emerging technologies and it is uncontroversial that human control, at some level, must be retained over AWS. The United States Air Force, for example, did not proceed with the development of a loitering weapon with a fully autonomous engagement mode, as it had concerns over controlling it.[301]

Higher level principles on control may, however, be more acceptable. The United States has several such policies, including that doctrine, tactics or procedures be established to ensure that AWS are sufficiently robust to minimise failures that could lead to a loss of control of the system, initiate unintended engagements and complete engagements in a timeframe consistent with a commander's intentions. If it is unable to do so, the United States policy provides that the AWS will seek to terminate engagements or seek additional human operator input before continuing the engagement.[302] To further ensure control, the policy provides that physical hardware and software will be designed with appropriate safeties and anti-tamper mechanisms.[303]

The critical distinction turns on what these two sets of principles are attempting to accomplish during AWS' development. The first attempts to achieve IHL compliance via impositions and restrictions. The second attempts to ensure human control without setting particular limits and, in the author's view, is likely to be much more palatable to widespread acceptance. The author therefore considers the following content, formed from the latter, could be added to the GGE's guiding principles, as set out in table 6:

Table 6:

Proposed additional content to the GGE guiding principles
a) To ensure reliability, security and prevent the loss of control of an autonomous weapon system to unauthorised parties, and consistent with the potential consequences of an unintended engagement, the physical hardware and software should be designed: a. With appropriate verification, validation, explainability, characterisation of failure conditions and behavioural specifications;

[301] Boulanin and Verbruggen, above n 21, at 54.
[302] DoD Directive, above n 11, at 2.
[303] DoD Directive, above n 11, at 2.

b. With safeties, anti-tamper mechanisms and information assurance;
c. With human-machine interfaces and controls;
d. To complete engagements in a timeframe consistent with commander and operator intentions and, if unable to do so, terminate engagements or seek additional human operator input before continuing the engagement; and
e. To be sufficiently robust to minimise failures that could lead to unintended engagements or to loss of control of the system to unauthorised parties.

5 General concerns with artificial intelligence when developing AWS

There is an inseverable link between AWS and the underlying technology or AI that allows these weapons to operate. Dr Angela Kane has raised a number of concerns with AI generally, that could impact on how these weapons operate.[304] These include problems with tendencies, discrimination and exclusion which are programmed into AI (whether intentionally or unintentionally), as well as algorithmic profiling of people and challenges in selecting data of quality, quantity and relevance.[305] Similarly, Paul Scharre, of the Center for a New American Security, warns AI has the potential to result in "millions of mistakes per second", similar to that seen with financial markets algorithms that resulted in the 2010 Dow Jones flash crash.[306] It is easy to see how similar outcomes could have catastrophic consequences on the battlefield.

These concerns have not been limited to scholars either, Russia's National Strategy for the Development of Artificial Intelligence recognises risks with AI when it acknowledged universal AI (similar to a human being), can lead to negative consequences.[307] Panama, in a submission to the GGE, raised concerns that AI has the potential to replicate human bias, such as discrimination, stereotypes and prejudice.[308]

To help mitigate these risks, Panama has suggested that developers be mindful of the implications of incomplete or inaccurate data.[309] Going further, the Campaign to Stop Killer Robots has proposed a requirement for certain minimum standards for predictability and reliability, when using an AI system.[310] To prevent disproportionate human reliance on AI, Sharkey proposes requiring certain levels of human control in the operation of AWS.[311] This

[304] Dr Angela Kane "Regulating AI: considerations that apply across domains" (29 May 2019) United Europe <www.united-europe.eu>.
[305] Kane, above n 304, quoting "How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence" (December 2017) Commission Nationale de l'Informatique et des Libertés, CNIL <www.cnil.fr>. See also Dahlmann and Dickow, above n 143, at 13.
[306] Paul Scharre "A Million Mistakes a Second" (12 September 2018) Foreign Policy <www.foreignpolicy.com>.
[307] Russia 2021 Working Paper, above n 2, at 4.
[308] Chairperson's Summary, above n 22, at 65.
[309] At 65.
[310] "Commentary for the Convention on Conventional Weapons Group of Governmental Experts on lethal autonomous weapons systems" (20 May 2020) Campaign to Stop Killer Robots <www.stopkillerrobots.org> at 4.
[311] Noel Sharkey "Guidelines for the human control of weapons systems" (April 2018) International Committee for the Robot Arms Control <www.icrac.net> at 3-4.

would prohibit any AWS that can identify, select and engage a target either fully by itself or with a human on-the-loop.[312]

Concerns around AI's effectiveness are undoubtably valid. Yet, while general statements like Russia's are easy to make, it is not so easy to distil these concerns into concrete proposals. This is particularly the case when much of this technology is still to be developed. Unfortunately, when proposals are put forward, they are often proposed as specific limitations or restrictions. Such specific limitations on how AI can be developed and used are very unlikely to gain widespread acceptance. Further, as much of this technology may be developed in the private sector, nor is it clear how effective any restrictions would actually be.

As this technology is developed and better understood, it is likely that more general and specific principles will be adopted. Yet, at this stage, it is unlikely states will accept a limitation of AI's development.

B The Risks Associated with Using AWS

Part IV of this dissertation provides that when AWS are eventually deployed and operated, they will need to comply with IHL's core assessments of distinction, proportionality and precautions in attack (amongst other requirements). These assessments will either need to be made by the AWS itself (which, in complex environments, appears unlikely for the foreseeable future), or left to humans to make these assessments.

Autonomous *features* in modern weapon systems are not only a reality, but are growing in prevalence.[313] Yet, as noted by Jeffrey Thurnher, it is the advent of autonomous lethal targeting capabilities that are drawing the most attention.[314] Critics argue that as these weapon systems increase in autonomy, humans will not be able to effectively use, operate or intervene to ensure that AWS can comply with IHL.[315] This could be because humans either do not understand how the weapons work or that the weapons will operate too quickly for a human to be able to meaningfully contribute or intervene.[316] Ensuring humans can effectively use AWS, therefore, should be a legal criterion. Critics also argue that the existence of AWS will encourage the practice of using large numbers or swarms of AWS, with little to no human involvement, which may result in an inability for these swarms to comply with IHL. A lack of human involvement may lead to unintended engagements.[317]

---

[312] At 3-4.
[313] For example, autonomy in drones, where certain drones have the ability to autonomously manoeuvre across the battlefield. See Thurnher, above n 100, at 178.
[314] Thurnher, above n 100, at 178.
[315] Sharkey, above n 311, at 4; and Docherty, above n 4, at 12.
[316] Anderson, Reisner and Waxman, n 107, at 394; and Vincent Boulanin, Neil Davison, Netta Goussac and Moa Peldan Carlsson "Limits on Autonomy in Weapon Systems: Identifying Practical Elements of Human Control" (June 2020) Stockholm International Peace Research Institute <www.sipri.org> at 21.
[317] Docherty, above n 4, at 29; and Sharkey, above n 53, at 183.

Unlike the Part above, which considers whether risks can be mitigated during the *development* of AWS, this Part considers whether, once developed and operational, there is anything that can be added to the GGE's guiding principles to ensure compliance with IHL during that weapon's use.

1 Requiring meaningful human control during the use and operation of AWS

As concluded above, in the author's opinion, specific requirements for meaningful human control in the *development* of AWS are unlikely to garner widespread acceptance anytime soon. A related but distinct argument is that AWS should only be allowed to be *used or operated* if there is appropriate human supervision over that operation.

Human involvement during the *use* of AWS has been addressed at the GGE meetings via principle (c):[318]

> Human-machine interaction, which may take various forms and be implemented at various stages of the life cycle of a weapon, should ensure that the potential use of weapons systems based on emerging technologies in the area of lethal autonomous weapons systems is in compliance with applicable international law, in particular IHL. In determining the quality and extent of human-machine interaction, a range of factors should be considered including the operational context, and the characteristics and capabilities of the weapons system as a whole.

What is unclear, however, is whether this principle is requiring human control over the *entire* lifecycle of the weapon system, or just over *aspects* of the weapon's lifecycle. The difference could mean human control is required over every "critical function" of an AWS' lifecycle, or just human control over the "trigger pull" decisions.[319]

Given the highly complex nature of AWS and its underlying technology and software, it has been argued that humans will not be able to understand AWS sufficiently to allow for appropriate compliance with IHL.[320] Boulanin and others argue that one human operator will not effectively be able to monitor the critical functions of AWS, and instead suggest multiple individuals need to be present.[321]

To have adequate human control, it is argued the human operator's understanding of the AWS needs to be sufficient to enable the prediction of the operation of a system and any foreseeable consequences in the specific circumstances of use.[322] Put more simply, what the system is going to do when, and why. A similar acknowledgement is made by the authors of the Roadmapping

---

[318] 2019 GGE Report, above n 33, guideline (c) at 13.
[319] "Convention on Certain Conventional Weapons (CCW) Lethal Autonomous Weapons Systems National Commentary – Australia" (paper submitted to the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, 2020) at 2; and Moyes, above n 82, at 2.
[320] Anderson, Reisner and Waxman, n 107, at 394.
[321] Boulanin and others, above n 316, at 21; Amoroso and Tamburrini, above n 237, at 27; and Boulanin, Bruun and Goussac, above n 78, at 16.
[322] Boulanin and others, above n 316, at 20.

Exercise, who note "humans responsible for initiating an attack must have sufficient understanding of the weapons, the targets, the environment and the context for use to determine whether that particular attack is lawful."[323] While the author does not disagree with this statement, or its sentiment, it is effectively a restatement of the information required to be able to comply with the current IHL regime (such as the proportionality and precautions in attack principles). An addition to the GGE principles is unnecessary, as it would simply be a replication of the existing law.

As also noted by Anderson, nor do soldiers and commanders necessarily need to understand exactly how a weapon system works to be able to operate within the confines of IHL.[324] Air force pilots, for example, are unlikely to know the precise inner workings of a jet fighter, yet they can appropriately operate it within the confines of IHL.

This is not to say, however, that soldiers should not be trained on how AWS work. On the contrary, it will be essential that they are. As highlighted by Dahlmann and Dickow, humans involved with these new weapon systems will be faced with significant amounts of data, and they will need to be trained to not get overwhelmed.[325] As also recognised by the authors of the Roadmapping Exercise, "militaries must invest in training, education, doctrine, policies, system design, and human-machine interfaces to ensure that humans remain responsible for attacks."[326] Waxman and Anderson also suggest guidance around training, which may include methodologies, operating procedures, rules of engagement and other operational and doctrinal level rules for the use of AWS.[327]

The importance of education for human operators is also recognised by the United States, which has a policy providing that:[328]

> In order for operators to make informed and appropriate decisions in engaging targets, the interface between people and machines for autonomous and semi-autonomous weapon systems shall be readily understandable to trained operators, provide traceable feedback on system status and provide clear procedures for trained operators to activate and deactivate system functions.

High level proposals to ensure effective control over AWS appears uncontroversial. It also does not constrain the parties by inhibiting development and therefore provides a balance between widespread acceptance and mitigation of risk. Additional content blending the United States policy and proposed education would, in the author's view, add significant value to GGE principle (c) and would likely have widespread acceptance. The author therefore considers the following content could be added to the GGE's guiding principles, as set out in table 7.

---

[323] Arkin and others, above n 233, at 6.
[324] Anderson, Reisner and Waxman, above n 107, at 394-395.
[325] Anja Dahlmann and Dickow, above n 143, at 13.
[326] Arkin and others, above n 233, at 6.
[327] Anderson, Reisner and Waxman, above n 107, at 408.
[328] DoD Directive, above n 11, at 2.

Table 7:

Proposed additional content to the GGE guiding principles
a) States shall ensure that human operators receive appropriate training and education and that there is appropriate methodologies, operating procedures, doctrine and policies to allow the weapon system to be operated in accordance with the law. b) In order for human operators to make informed and appropriate decisions in engaging targets, the interface between people and machines for autonomous weapon systems shall be: a. readily understandable to trained operators; b. provide traceable feedback on system status; and c. provide clear procedures for trained operators to activate and deactivate system functions.

2 Imposing restrictions on the use of AWS to ensure compliance with IHL

When, where and how any weapon system, including AWS, can be used in accordance with IHL will always be a case-by-case analysis, to be determined on its distinct set of facts. This is inherent in the judgement-based assessments of distinction, proportionality and precautions in attack.

Yet scholars have suggested that best-practice interpretive guidance can greatly assist with compliance of IHL. Waxman and Anderson, for example, note that interpretive application could be included in guidance, such as explaining what information commanders would need to have and what questions they must ask before deciding to field the weapons in a given situation.[329] Alternatively, this guidance could take the form or restrictions or limitations, seeking to mitigate certain risks.

Practical guidance on the use of AWS could generally fall into three separate categories; guidance on "when" AWS could be used, "where" AWS could be used and "how" AWS could be used. The authors of the Roadmapping Exercise suggest that in order for a determination about the lawfulness of an attack to be meaningful, requirements could be established to ensure any attack must be bounded in space (where AWS should be used), time (when AWS should be used), target class and means of attack (how AWS should be used).[330] It is argued that these regulations will ensure the maximum level of compliance with IHL. Yet, given these restrictions would be imposed via soft law, it would be up to states to comply with them and there is no real means of enforcement.

Operational restraints, regulating *when* AWS can be used, include proposals to limit AWS to certain missions[331] or requiring rules for autonomous system behaviour when in proximity to adversarial forces, to avoid any unintentional escalation or signalling. Other restrictions or

[329] Anderson, Reisner and Waxman, above n 107, at 407.
[330] Arkin and others, above n 233, at 6.
[331] Williams, above n 207, at 180; and Combe, above n 111, at 53.

requirements on when AWS should be used or deployed include the weather, the lethality of the system, imposing certain escalation measures, whether a stationary or non-stationary system is more appropriate or whether the offensive and defensive abilities exceed certain pre-established parameters.[332]

From a geographical or spatial perspective, which focuses on *where* AWS can be used, John Lewis suggests there could be geographical or spatial criteria or restrictions such that AWS could only be used in certain areas. This would be similar to the land mines protocol in the CCW, where mines are prohibited from use in areas dedicated to civilian areas.[333] Similarly, the deployment of AWS could be prohibited from certain areas/situations, such as densely populated areas, schools or places of worship.

There have been a number of proposals around *how* AWS should be used. Explicit restrictions have been proposed around deployment of AWS, such that deployment could only occur when the enemy are using certain insignia and where countermeasures are not being undertaken (noting the AWS' capabilities or ability to distinguish). There could also be a limits on the commander's actions, similar to the CCW protocol on mines, with associated sanctions on those who do not comply.[334] An AWS "no-first-fire" policy could be imposed, so that AWS do not initiate hostilities without explicit human authorisation.[335] The targets of AWS could be restricted, such that AWS could only be used to attack non-human targets.[336] Alternatively, for human targets, there could be a requirement that AWS only be equipped with non-lethal capabilities (such as pepper sprays, optical dazzlers or active denial systems).[337] There could also be requirements on the quantity of AWS being used, to ensure no command or control is lost (this links to corresponding capacities for human in-the-loop operation of those weapons).[338]

Focussing on the adversary, requirements for states to take steps to clearly distinguish exercises, patrols, reconnaissance, or other peacetime military operations, from attacks, could limit the possibility of reactions from adversary autonomous systems (such as autonomous air or coastal defenses).[339] Militaries could be prevented from jamming others' ability to recall their autonomous systems, in order to afford the possibility of human correction in the event of unauthorised behaviour.[340]

An alternative approach from the Canberra Working Group, proposes a risk-based authorisation system for using AWS. Where the higher the risks from using that AWS in a

---

[332] Lewis, above n 52, at 1324; and Combe, above n 111, at 58-59.
[333] Lewis, above n 52, at 1321.
[334] At 1324.
[335] Arkin and others, above n 233, at 7.
[336] Boulanin and others, above n 316, at 14.
[337] Combe, above n 111, at 58.
[338] Arkin and others, above n 233, at 7.
[339] At 7.
[340] At 7.

particular context are, then the higher the chain of command authority is needed.[341] This authority could extend beyond the military to the top of the political leadership.

The GGE has tentatively approached the issue of restrictions, with guiding principle (h): "Consideration should be given to the use of emerging technologies in the area of lethal autonomous weapons systems in upholding compliance with IHL and other applicable international legal obligations."[342] In effect, however, this is simply a requirement for states to comply with IHL. The United States, with a policy in its directive, has effectively done the same thing.[343] While it does provide some operational guidance, this really just authorises the United States' current practice involving existing semi-autonomous weapon systems (or autonomous features within these weapon systems).

Notably, what can be drawn from the United States' policies, is that while they authorise certain activities with certain weapons, no explicit activities are prohibited, restricted or limited. This highlights how unlikely it is that states will agree to any specific requirements for when, where and how AWS may be used. It could even be argued that restrictions could impede compliance with IHL, as scenarios are envisioned where restrictions prevent certain AWS from operating; where those systems could actually out-perform human performance.

It is notable that many of the proposed restrictions set out above closely follow restrictions seen in current treaties (such as the CCW protocol on anti-personnel mines). Yet, these treaties relate to technology and capabilities that are currently understood. It is likely to be some years before we understand the capabilities of AWS, and indeed we may never reach some of the thresholds currently envisioned. As technology develops and capabilities are better understood, it is likely that militaries will continue to develop operational guidelines and standard operating procedures. In the same manner that operational guidelines assist with other existing technologies, such as land mines or even in the cyber space. Yet, in the author's view, until this technology is developed, it is unlikely that any restrictions or limitations will be widely accepted and they will be seen to inhibit the development of this technology. Accordingly, this dissertation does not propose to add any content to the GGE's guiding principle (h).

IX Conclusion

This dissertation begins by posing a dilemma; are several large states holding the world hostage by purposely preventing the challenges raised by AWS from being addressed, or is a coalition of well-intentioned states and organisations preventing the development of weapons that may *increase* compliance with IHL? In the author's opinion, there is truth in both of these positions.

---

[341] Baker and others, above n 275, at 4.
[342] 2019 GGE Report, above n 33, guideline (h) at 13.
[343] DoD Directive, above n 11, at 3.

Yet, these diametric positions do not prevent us from immediately doing something about it. On the contrary, the GGE has already provided us with a foundation to be built upon.

As set out in Part IV, in many circumstances, AWS will undoubtably create challenges for compliance with IHL. Yet, there does not appear to be a strong basis for a pre-emptive ban on the development or use of AWS due to their inability to comply with the core IHL principles.

Further, despite the loud calls by critics, a new treaty prohibiting AWS which would receive widespread acceptance is, in the author's view, unrealistic. The international context to date has made this very clear. Significant amounts of time and money are being invested to develop this technology as quickly as possible. While there is nothing stopping the remaining states negotiating a treaty absent these dissenters, this is likely to have limited value given the states developing the AWS are unlikely to be part of it. This is similar to what has occurred with the TPNW. For similar reasons, the current international context means is it unlikely that customary international law is a viable option to address AWS' challenges. A quasi-legal mechanism like Resolution 1540 may well be a valuable mechanism at some stage, yet, as AWS technology is still developing, any similar mechanism is unlikely to be implemented in the near future.

This leaves soft law as the best solution to both address the challenges raised by AWS and receive widespread acceptance. The GGE principles, themselves a form of soft law, have already been agreed by consensus and have created a foundation to be built upon. Yet, as critics are quick to point out, they do not go far enough to address the challenges created by AWS. This dissertation therefore recommends adding additional content to the GGE's guiding principles.

The additional content proposed by this dissertation attempts to balance respect for IHL, while achieving widespread acceptance. This balance often means guidelines that address specific IHL concerns must be omitted, as they are unlikely to receive broad support. This is particularly relevant to many of the restrictions and limitations proposed by states, organisations and scholars to address bespoke IHL concerns. For example, while many of the restrictions proposed will likely assist AWS to comply with IHL's targeting laws, they are unlikely to be accepted as they may inhibit AWS' development. Similarly, imposing requirements for meaningful human control are unlikely to gain widespread acceptance. Instead, higher level guidelines, similar to those already agreed at the GGE meetings, are most likely to achieve this widespread support.

This dissertation concludes that considerable value can nonetheless be gained from adding additional content to the GGE guiding principles. This includes, while still at a high level to promote acceptance, more focussed and context specific guidance to ensure accountability when developing and using AWS. More prescriptive guidance for conducting weapon reviews with autonomous technology would also significantly assist to ensure these weapons are being fully and accurately assessed for compliance with IHL. Significant value can also be obtained

from high level guidance around weapon design, which goes much further than the current GGE guiding principles. Lastly, guidance on training and education would assist to ensure that AWS can be operated in an appropriate manner, while minimising the risks of unintended consequences. This would go much further than the existing, higher level, GGE principles and seek to address many of the concerns that critics are raising.

The content of any set of soft law guidelines will always be subject to dispute. They will either be seen as being too broad and high level, with minimal value being added to any challenges raised; or specific, but with little chance of actually being accepted by the states developing these weapons. Critics are also likely to point out that compliance with these soft law guidelines is left to individual states, with no means of enforcement. Yet, there has already been buy-in from states to the GGE's guiding principles, which were accepted by consensus. It is therefore reasonable to expect similar buy-in to an extension of these principles. As noted above, partial compliance will always be more beneficial to no compliance, which, in the author's view, is what is likely to occur under any other mechanism.

The solution proposed by this dissertation is not made without respect for IHL. On the contrary, Part IV, and indeed the GGE itself, recognises that there is an existing IHL regime that applies fully to AWS. Indeed, there is a strong argument that, in certain circumstances, AWS will actually *promote* compliance with IHL. The additional content proposed by this dissertation aims to assist with this existing IHL regime. While AWS will undoubtably create challenges, the soft law solution proposed is, in the author's view, the best way of mitigating these challenges.

Finally, there is also one further benefit of soft law guidelines. Not only do they provide utility now, mitigating many of the challenges we currently and in the future will face, but they also provide a useful point to return to once this technology has developed further and is better understood. Just because a bespoke solution is not likely to be generally agreeable now, does not mean it will not be in several years' time, when we have a greater understanding of the implications of such a bespoke solution. Guidelines are, in this sense, fluid, able to be refined and developed further as the understanding of technology develops. Yet, they nevertheless provide the most realistic and pragmatic solution to address the current challenges we are facing from AWS.

X Bibliography

PRIMARY SOURCES

A Cases

North Sea Continental Shelf (Federal Republic of Germany v Denmark; Federal Republic of Germany v Netherlands) [1969] ICJ Rep 3.

B Treaties, Conventions and Resolutions

Additional Protocol to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects (Protocol IV, entitled Protocol on Blinding Laser Weapons) 1380 UNTS 370 (opened for signature 10 April 1981, entered into force 30 July 1998).

Arms Trade Treaty 52 ILM 988 (opened for signature 3 June 2013, entered into force 24 December 2014).

Convention on Cluster Munitions 2688 UNTS 39 (opened for signature 3 December 2008, entered into force 1 August 2010).

Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects 1342 UNTS 137 (opened for signature 10 October 1988, entered into force 2 December 1983).

Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and their Destruction 2056 UNTS 211 (opened for signature 3 December 1997, entered into force 1 March 1999).

Convention Respecting the Laws and Customs of War on Land (Hague Convention IV) 205 CTS 277 (opened for signature 18 October 1907, entered into force 26 January 1910).

Project of an International Declaration concerning the Laws and Customs of War, Brussels, 27 August 1874 (Brussels Declaration).

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) 1125 UNTS 3 (opened for signature 8 June 1977, entered into force 7 December 1978).

Regulations Respecting the Laws and Customs of War on Land annexed, respectively, to Hague Convention II of 29 July 1899.

Treaty on the Prohibition of Nuclear Weapons (opened for signature 20 September 2017, entered into force 22 January 2021).

United Nations Security Council Resolution 1540 SC Res 1540 (2004).

Vienna Convention on the Law of Treaties 1155 UNTS 331 (opened for signature 23 May 1969, entered into force 27 January 1980).

SECONDARY SOURCES

C Books and Chapters in Books

Alberto Costi, Scott Davidson and Lisa Yarwood "The Creation of International Law" in Alberto Costi (ed) *Public International Law: A New Zealand Perspective* (LexisNexis, Wellington, 2020).

Alberto Costi (ed) *Public International Law: A New Zealand Perspective* (LexisNexis, Wellington, 2020).

David Mindell *Our Robots, Ourselves: Robotics and the Myths of Autonomy* (Viking, New York, 2015).

Gary D Solis *The Law of Armed Conflict: International Humanitarian Law in War* (2nd ed, Cambridge University Press, New York, 2016).

Harvard University Humanitarian Policy and Conflict Research *Manual on International Law Applicable to Air and Missile Warfare* (Cambridge University Press, Cambridge, 2013).

Jean-Marie Henckaerts and Louise Doswald-Beck *ICRC Customary International Humanitarian Law Volume I: Rules* (Cambridge University Press, Cambridge, 2005).

Jeffrey S Thurnher "Means and Methods of the Future: Autonomous Weapon Systems" in Paul AL Ducheine, Michael N Schmitt and Frans PB Osinga (ed) *Targeting: The Challenges of Modern Warfare* (T.M.C. Asser Press, The Hague, 2016).

Kenneth Anderson and Matthew Waxman "Debating Autonomous Weapon Systems, their ethics, and their regulation under International Law" in Roger Brownsword, Eloise Scotford

and Karen Yeung *The Oxford Handbook of Law, Regulation and Technology* (Oxford University Press, Oxford, July 2017).

Kevin Riordan "The Law of Armed Conflict" in Alberto Costi (ed) *Public International Law: A New Zealand Perspective* (LexisNexis, Wellington, 2020).

Louise Doswald-Beck *San Remo Manual on International Law Applicable to Armed Conflicts at Sea* (Cambridge University Press, Cambridge, 1995).

Michael N Schmitt (ed) *Tallinn Manual on the International Law Applicable to Cyber Warfare: prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge University Press, Cambridge, 2013).

Rebecca Crootof "Regulating New Weapon Technologies" in Ronald T P Alcala and Eric Talbot Jensen (ed) *The Impact of Emerging Technologies on the Law of Armed Conflict* (Oxford University Press, New York, 2019).

William H Boothby *New technologies and the law in war and peace* (Cambridge University Press, Cambridge, 2019).

Yoram Dinstein and Arne Dahl "Remote and Autonomous Weapons" in Yoram Dinstein and Arne Dahl *Oslo Manual on Select Topics of the Law of Armed Conflict* (Springer International Publishing, Switzerland, 2020)

Yoram Dinstein *War Aggression and Self-Defence* (6th ed, Cambridge, Cambridge University Press, 2017).

D Journal Articles

Amitai Etzioni and Oren Etzioni "Pros and Cons of Autonomous Weapons Systems" (May-June 2017) 97 Military Review 72.

Andrew Guzman and Timothy Meyer "International Soft Law" (Spring 2010) 2 Journal of Legal Analysis 171.

Angelo Bellis, Phil Torres and Steven Umbrello "The future of war: could lethal autonomous weapons make conflict more ethical?" (6 February 2019) 35 AI and Society 273.

Austin Wyatt "Charting great power progress toward a lethal autonomous weapon system demonstration point" (2020) 20 Defence Studies 1.

Ben Paxton “2017 saw 122 countries – but none of the nuclear weapon states – support the treaty for the prohibition of nuclear weapons. Why is nuclear disarmament so difficult and what should be the next steps for those aiming for prohibition?” (2019) 35 Medicine, Conflict and Survival 336.

Charles Trumbull IV “Autonomous Weapons: How existing law can regulate future weapons” (2020) 34 Emory International Law Review 533.

Christopher W Jacobs “Taking the next step: an analysis of the effects of the Ottawa Convention may have on the interoperability of the United States Forces with the Armed Forces of Australia, Great Britain and Canada” (2004) 180 MIL L Rev 49.

Daniele Amoroso and Guglielmo Tamburrini “In search of the ‘Human Element’: International Debates on Regulating Autonomous Weapon Systems” (2021) 56 The International Spectator 20.

Elvira Rosert and Frank Sauer “Prohibiting Autonomous Weapons: Put Human Dignity First” (2019) 10 Global Policy 370.

Frank Sauer “Stepping back from the brink: Why multilateral regulation of autonomy in weapons systems is difficult, yet imperative and feasible” (2020) 102 International Review of the Red Cross 235.

Jan Klabbers “The undesirability of soft law” (January 1998) 67 Nordic Journal of International Law 381.

John Lewis “The Case for Regulating Fully Autonomous Weapons” (2015) 124 The Yale Law Journal 1309.

John Williams “Democracy and Regulating Autonomous Weapons: Biting the Bullet while Missing the Point?” (2015) 6 Global Policy 179.

Karen Hulme “The 2008 Cluster Munitions Convention: Stepping Outside the CCW Framework (Again)” (2009) 58 ICLQ 219.

Kathleen Lawland “A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977” (December 2006) 88 International Review of the Red Cross 931.

Kenneth Anderson, Daniel Reisner and Matthew Waxman “Adapting the Law of Armed Conflict to Autonomous Weapon Systems” (2014) 90 International Law Studies 386.

Kenneth Anderson “The Ottawa Convention Banning Landmines, the Role of International Non-governmental Organisations and the Idea of International Civil Society” (2000) 11 EJIL 91.

Kenneth Anderson “Why the Hurry to Regulate Autonomous Weapon Systems – But Not Cyber Weapons” (2016) 30 Temp Int’l & Comp L.J. 17.

Karen M Feigh and Amy R Pritchett “Requirements for effective function allocation: A critical review” (2014) 8 J Cognitive Engineering and Decision Making 1 as cited in Marc Cannellos and Rachel Haga “Lost in Translation: Building a Common Language for Regulating Autonomous Weapons” (9 September 2016) 35 IEEE Technology and Society Magazine 50.

Laurence R Helfer and Ingrid B Wuerth “Customary International Law: An Instrument Choice Perspective” (2016) 37 Michigan Journal of International Law 563.

Louise Doswald-Beck “New Protocol on Blinding Laser Weapons” (30 June 1996) 312 International Review of the Red Cross 272.

Marc Cannellos and Rachel Haga “Lost in Translation: Building a Common Language for Regulating Autonomous Weapons” (9 September 2016) 35 IEEE Technology and Society Magazine 50.

Metodi Hadji-Janev and Kiril Hristovski “Beyond the Fog: Autonomous weapon systems in the context of the international law of armed conflicts (Symposium on Governance of Emerging Technologies: Law, Policy, and Ethics)” (2017) 57 Jurimetrics Journal of Law Science and Technology 325.

Michael N Schmitt and Jeffrey S Thurnher ““Out of the Loop”: Autonomous Weapon Systems and the Law of Armed Conflict” (2013) 4 Harvard National Security Journal 231.

Noel Sharkey “Saying ‘No!’ to Lethal Autonomous Targeting” (2010) 9 Journal of Military Ethics 369.

Noel Sharkey “Why robots should not be delegated with the decision to kill” (2017) 29 Connection Science 177.

Peter Combe "Autonomous Doctrine: Operationalising the Law of Armed Conflict in the Employment of Lethal Autonomous Weapon Systems" (2020) 51 St. Mary's Law Journal 35.

Peter Crail "Implementing UN Security Council Resolution 1540: A Risk-Based Approach" (2006) 13 Nonproliferation Review 355.

E Unpublished Papers, Reports and Working Papers

"Agenda item 5(e)" (New Zealand Statement to the Group of Governmental Experts, Geneva, 27 March 2019).

"Australia's System of Control and applications for Autonomous Weapon Systems" (working paper to the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, 20 March 2019).

"Chairperson's Summary" (Chairperson's summary of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, 19 April 2021).

"Convention on Certain Conventional Weapons (CCW) Lethal Autonomous Weapons Systems National Commentary – Australia" (paper submitted to the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, 2020).

"Draft Agenda" (draft agenda for the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, September 2020).

"ICRC commentary on the 'Guiding Principles' of the CCW GGE on 'Lethal Autonomous Weapon Systems'" (paper submitted to the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, July 2020).

"International humanitarian law and the challenges of contemporary armed conflicts: Report prepared for the 32nd International Conference of the Red Cross and Red Crescent" (ICRC report prepared for the 32nd International Conference of the Red Cross and Red Crescent, 8-10 December 2015).

"Israel Considerations on the Operationalisation of the Eleven Guiding Principles Adopted by the Group of Governmental Experts" (Paper submitted to the Group of Governmental Experts, Geneva, 31 August 2020).

"Joint 'Commentary' on Guiding Principles A, B, C and D" (Paper submitted to the Group of Governmental Experts, Geneva, 2020).

Joseph Ballard "Statement by Joseph Ballard Deputy Permanent Representative to the Conference on Disarmament" (New Zealand Statement to the Informal Meeting of Experts on Lethal Autonomous Weapon Systems, Geneva, 13 May 2014).

Katy Donnelly "Statement by Katy Donnelly Deputy Permanent Representative to the Conference on Disarmament, Geneva" (New Zealand Statement to the Group of Governmental Experts, Geneva, 13 April 2018).

Laurent Gisel "The principle of proportionality in the rules governing the conduct of hostilities under International Humanitarian Law" (report prepared by the ICRC and University Laval for the International Expert Meeting, 22-23 June 2016, Quebec).

"National commentaries on the 11 guiding principles – Comments by Italy" (Paper submitted to the Group of Governmental Experts, Geneva, 2020).

"New Zealand Statement" (New Zealand Statement to the Meeting of Experts on Lethal Autonomous Weapon Systems, Geneva, 2016).

"New Zealand Statement on Lethal Autonomous Weapons Systems" (paper submitted to the Meeting of High Contracting Parties on the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, Geneva, 2018).

"Non-paper by the GGE Chair" (working paper to the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, March 2020).

"Pre-Feasibility Study on UAV Autonomous Operations" (NATO Industrial Advisory Group Study Group 75, study paper of the NATO Industrial Advisory Group, 2004).

"Proposal for a Mandate to Negotiate a Legally binding Instrument that addresses the Legal, Humanitarian and Ethical Concerns posed by Emerging Technologies in the Area of Lethal Autonomous Weapons Systems" (working paper to the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, 30 August 2018).

"Recommendations to the 2016 Review Conference" (working paper to the Informal Meeting of Experts, Geneva, December 2016).

"Report of the 2019 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems" (final report of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, 25 September 2019).

"Statement to the Informal Meeting of Experts on Lethal Autonomous Weapon Systems" (United Kingdom of Great Britain and Northern Ireland Statement to the Informal Meeting of Experts on Lethal Autonomous Weapon Systems, 11-15 April 2016).

"The Australian Article 36 Review Process" (working paper to the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, 30 August 2018).

"UK Commentary on the Operationalisation of the LAWS Guiding Principles" (Paper submitted to the Group of Governmental Experts, Geneva, 2020).

"Working Paper of the Russian Federation: National Implementation of the Guiding Principles on Emerging Technologies in the Area of Lethal Autonomous Weapon Systems" (Paper submitted to the Group of Governmental Experts, Geneva, 2020).

F Media Reports, Press/News Releases and Letters

Letter from Annabel Jenkin (Conventional Arms Policy Officer) to Natalie Samarasinghe and Richard Moyes (Executive directors, United Nations Association) regarding the United Kingdom's definition of lethal autonomous weapon systems (8 December 2017).

Letter from Marc Pecsteen (Ambassador of Belgium and Chair of the GGE) to the high contracting parties of the CCW regarding a request for recommendations at the 2021 GGE meetings (26 April 2021).

Letter from Winston Peters (Minister of Foreign Affairs) to Mary Wareham (Coordinator, Campaign to Stop Killer Robots) regarding New Zealand's position on LAWS (1 May 2019).

G Internet Materials and Podcasts

"5. Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction" (27 December 2020) United Nations <www.treaties.un.org>.

"6. Convention on Cluster Munitions" (27 December 2020) United Nations <www.treaties.un.org>.

"2014 Meeting of Experts on Lethal Autonomous Weapons Systems" (2014) United Nations <www.unog.ch>.

"Additional Protocol to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects: Text with amendments and protocols adopted through 28 November 2003" (June 2005) International Committee of the Red Cross <www.icrc.org>.

"Airpower Teaming System" (2021) Boeing <www.boeing.com>.

Alice Black and Daan Kayser "Convergence? European positions on lethal autonomous weapon systems Update 2019" (November 2019) PAX for Peace <www.paxforpeace.nl>.

Alice Beck, Daan Kayser and Frank Slijper "State of AI, Artificial Intelligence, the military and increasingly autonomous weapons" (April 2019) PAX for Peace <www.paxforpeace.nl>.

"All action and achievements" (undated) Campaign to Stop Killer Robots <www.stopkillerrobots.org>.

Anja Dahlmann and Marcel Dickow "Preventative Regulation of Autonomous Weapon Systems" (March 2019) German Institute for International and Security Affairs <www.swp-berlin.org>.

Anna Bacciarelli "Artificial intelligence: the technology that threatens to overhaul our rights" (20 June 2017) Amnesty International <www.amnesty.org>.

"Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons" (15-16 March 2016) International Committee of the Red Cross <www.icrc.org>.

"Autonomous weapons that kill must be banned, insists UN chief" (25 March 2019) United Nations <www.news.un.org>.

Bonnie Docherty “Heed the Call: A Moral and Legal Imperative to Ban Killer Robots” (August 2018) Human Rights Watch <www.hrw.org>.

Bonnie Docherty “Making the Case: The dangers of killer robots and the need for a pre-emptive ban” (December 2016) Human Rights Watch <www.hrw.org>.

“Commentary for the Convention on Conventional Weapons Group of Governmental Experts on lethal autonomous weapons systems” (20 May 2020) Campaign to Stop Killer Robots <www.stopkillerrobots.org>.

“Convention on Certain Conventional Weapons (CCW)” (2020) United Nations Mine Action Service <www.unmas.org>.

“Country Views on Killer Robots” (25 October 2019) Campaign to Stop Killer Robots <www.stopkillerrobots.org>.

Daan Kayser and Stepan Denk “Keeping Control: European positions on lethal autonomous weapon systems” (12 November 2017) PAX for Peace <www.paxforpeace.nl>.

Daniel Edelstein “Potential Gains for Israel After Azerbaijan’s Victory in Nagorno-Karabakh” (10 March 2021) Just Security <www.justsecurity.org>.

Deane-Peter Baker and others “Guiding Principles for the Development and Use of LAWS Version 1.0” (April 2019) E-International Relations <www.e-ir.info>.

Dr Angela Kane “Regulating AI: considerations that apply across domains” (29 May 2019) United Europe <www.united-europe.eu>.

Eric Schmidt and others “Final Report: National Security Commission on Artificial Intelligence” (March 2021) National Security Commission on Artificial Intelligence <www.nscai.gov>.

Erin Hunt “Stigmatizing Cluster Munitions: A Decade of Success” (October 2020) Arms Control Association <www.armscontrol.org>.

Esther Chavannes, Klaudia Klonowska and Tim Sweijs “Governing Autonomous Weapon Systems” (17 March 2020) The Hague Centre for Strategic Studies <www.hcss.nl>.

Ewen Levick “Boeing’s Autonomous Fighter Jet Will Fly Over the Australian Outback” (2020) IEEE Spectrum <www.spectrum.ieee.org>.

Franz-Stefan Gady “Russia’s New Nuclear Torpedo-Carrying Sub to Begin Sea Trials in June 2020” (10 September 2019) The Diplomat <www.thediplomat.com>.

Hans Kristensen and Matt Korda “The Treaty on the Prohibition of Nuclear Weapons Enters Into Force Today” (22 January 2021) Federation of American Scientists <www.fas.org>.

Heather Roff “The Ontology of Autonomy for Autonomous Weapon systems” (Podcast, 5 April 2017) University of Oxford <www.podcasts.ox.ac.uk>.

“High contracting parties and signatories” (17 June 2020) United Nations <www.unog.ch>.

Hon Phil Twyford “Workshop on Lethal Autonomous Weapons Systems - opening remarks” (14 April 2021) The Beehive <www.beehive.govt.nz>.

“How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence” (December 2017) Commission Nationale de l’Informatique et des Libertés, CNIL <www.cnil.fr>.

Hugo Klijn and Maaike Okano-Heijmans “Managing RAS: The Need for New Norms and Arms Control” (17 March 2020) The Hague Centre for Strategic Studies <www.hcss.nl>.

“ICRC position on autonomous weapon systems” (12 May 2021) International Committee of the Red Cross <www.icrc.org>.

Kelley M Sayler “Defence Primer: U.S. Policy on Lethal Autonomous Weapon Systems” (19 December 2019) Congressional Research Service <www.crsreports.congress.gov>.

Kyle Mizokami “Trump’s 'Super Duper Missile' Is Actually Super Duper Real” (20 July 2020) Popular Mechanics <www.popularmechanics.com>.

Mary Wareham “Statement by the Campaign to Stop Killer Robots to the Convention on Conventional Weapons” (22 November 2018) Human Rights Watch <www.hrw.org>.

“Minority of states block progress on regulating killer robots” (4 September 2018) United Nations Association UK <www.una.org.uk>.

“Minority of states delay effort to ban killer robots” (29 March 2019) Campaign to Stop Killer Robots <www.stopkillerrobots.org>.

Neil C Renic “Autonomous Weapon Systems: When is the time to regulate?” (26 September 2019) International Committee of the Red Cross <www.icrc.org>.

"New robot has crown-of-thorns starfish in its sights" (2 September 2015) Queensland University of Technology <www.qut.edu.au>.

Noel Sharkey "Guidelines for the human control of weapons systems" (April 2018) International Committee for the Robot Arms Control <www.icrac.net>.

"Notice of the State Council Issuing the New Generation of Artificial Intelligence Development Plan" (July 2017) The Foundation for Law and International Affairs <www.flia.org>.

"Open lesson "Russia, aspiring to the future"" (1 September 2017) President of Russia <www.kremlin.ru>.

"Organisation for Security and Cooperation in Europe: Annual Report 2018" (2018) Organisation for Security and Cooperation in Europe <www.osce.org>.

Pablo Olabuenaga "Why the Arms Trade Treaty Matters – and Why It Matters That the US Is Walking Away" (8 May 2019) Just Security <www.justsecurity.org>.

Pablo Robles "China plans to be a world leader in Artificial Intelligence by 2030" (1 October 2018) South China Morning Post <www.scmp.com>.

Patrick Tucker "Russia to the United Nations: Don't Try to Stop Us From Building Killer Robots" (21 November 2017) Defence One <www.defenseone.com>.

Paul Iddon "The Last Azerbaijan-Armenia War Changed How Small Nations Fight Modern Battles" (25 March 2021) Forbes <www.forbes.com>.

Paul Scharre "A Million Mistakes a Second" (12 September 2018) Foreign Policy <www.foreignpolicy.com>.

"Report on a European Parliament recommendation to the Council on the 73rd session of the United Nations General Assembly (2018/2040(INI))" (27 June 2018) European Parliament <www.europarl.europa.eu>.

Richard Moyes "Autonomy in weapons systems – considering approaches to regulation" (March 2020) Article 36 <www.article36.org>.

Richard Moyes "Critical Commentary on the "Guiding Principles"" (November 2019) Article 36 <www.article36.org>.

Robyn Dixon “Azerbaijan’s drones owned the battlefield in Nagorno-Karabakh - and showed future of warfare” (11 November 2020) The Washington Post <www.washingtonpost.com>.

Ronald Arkin and others “Autonomous Weapon Systems: A Roadmapping Exercise” (9 September 2019) Georgia Institute of Technology <www.cc.gatech.edu>.

“Stopping Killer Robots: Country Positions on Banning Fully Autonomous Weapons and Retaining Human Control” (10 August 2020) Campaign to Stop Killer Robots <www.stopkillerrobots.org>.

Ted Piccone “How can international law regulate autonomous weapons?” (10 April 2018) Brookings <www.brookings.edu>.

“The FY 2020 Budget Request: Security R&D” (23 April 2019) American Association for the Advancement of Science <www.aaas.org>.

“Treaty on the Prohibition of Nuclear Weapons” (11 December 2020) United Nations <www.treaties.un.org>.

“US has 'moral imperative' to develop AI weapons, says panel” (26 January 2021) The Guardian <www.theguardian.com>.

Vincent Boulanin, Laura Bruun and Netta Goussac “Autonomous Weapon Systems and International Humanitarian Law” (June 2021) Stockholm International Peace Research Institute <www.sipri.org>.

Vincent Boulanin and Maaike Verbruggen “Mapping the Development of Autonomy in Weapon Systems” (November 2017) Stockholm International Peace Research Institute <www.sipri.org>.

Vincent Boulanin, Neil Davison, Netta Goussac and Moa Peldan Carlsson “Limits on Autonomy in Weapon Systems: Identifying Practical Elements of Human Control” (June 2020) Stockholm International Peace Research Institute <www.sipri.org>.

H Government Materials

British Ministry of Defence “Unmanned Aircraft Systems” (August 2017) Joint Doctrine Publication 0.30.2.

New Zealand Defence Force “Manual of Armed Forces Law: Commander’s Handbook on Military Law DM 69 (2 ed) Volume 4 Law of Armed Conflict” (20 June 2020).

United States Department of Defense “Autonomy in Weapon Systems” (21 November 2012, updated 8 May 2017) Directive 3000.09.