INTERNATIONAL LAW STUDIES

Published Since 1895

Autonomy and Precautions in the Law of Armed Conflict

Eric Talbot Jensen

96 INT'L L. STUD. 577 (2020)

Volume 96

2020

Published by the Stockton Center for International Law

ISSN 2375-2831

Autonomy and Precautions in the Law of Armed Conflict

Eric Talbot Jensen[*]

CONTENTS

* Professor of Law, Brigham Young University Law School. The author would like to thank Summer Crockett and Carolyn Sharp for excellent research and review assistance.

This article originated from a NATO Cooperative Cyber Defence Centre of Excellence project examining autonomous cyber capabilities. It and other papers produced during the project will appear in AUTONOMOUS CYBER CAPABILITIES UNDER INTERNATIONAL LAW (Rain Liivoja & Ann Väljataga eds., forthcoming 2021).

The thoughts and opinions expressed are those of the author and not necessarily those of the U.S. government, the U.S. Department of the Navy, or the U.S. Naval War College.

I. INTRODUCTION

Fixating on what amount of human control is required in the employment of autonomous weapons, including autonomous cyber capabilities, erroneously disregards the most important question with respect to autonomy in armed conflict. The question is whether autonomous weapons can "select" and "attack" targets in a manner that complies with the law of armed conflict (LOAC).[1] Some argue that to comply with the LOAC, selecting and targeting *requires* human judgment. There is no consensus on that assertion. Indeed, States that are Parties to the Certain Conventional Weapons Convention (CCW) have not acknowledged that human involvement in selecting and engaging targets is required under the LOAC.[2] Rather, the views of States vary widely on this issue, precluding the assertion that there is a current prohibition.

This article analyzes the specific LOAC rules on precautions in attack, as codified in Article 57 of Additional Protocol I (AP I) and asserts that these rules do not require human judgment in targeting decisions. Rather, these rules prescribe a particular analysis that must be completed. That analysis is one, which, in the future, may be done just as effectively (if not more effectively) by weapons systems using autonomous functions.

Part II of this article briefly discusses what "autonomy" means and highlights that there is no single agreed-upon definition. For the purposes of this

---

1. For purposes of this article, I will use LOAC and IHL interchangeably, though I recognize that some may argue that they are different in both content and approach to regulation during armed conflict.

2. One example is the Israeli Harpy NG. According to Shelby Smith,

> One example of an autonomous weapon system is the loitering munition. Loitering munitions, which hover over a human-designated area and strike at targets that match specific parameters, are currently only employed in Israel. The *Harpy NG*, the most commonly used and advanced model manufactured by Israel Aerospace Industries, is designed to attack enemy radar systems. These loitering munitions resemble drones, or UAVs, and can stay in the air for up to nine hours. Because loitering munitions are set up with specific limits to their range, they may offer a model for future development of autonomous weapons that afford an element of control without the need for human monitoring.

Shelby Smith, *Automated Defense Technology*, 3 GEORGETOWN LAW TECHNOLOGY REVIEW 492, 499 (2019). Other systems include the Counter-Rocket Artillery Mortar (C-RAM) and the Phalanx. *See Counter-Rocket Artillery Mortar (C-RAM) Intercept Land-Based Phalanx Weapon System (LPWS)*, U.S. ARMY, https://asc.army.mil/web/portfolio-item/ms-c-ram_lpws/ (last visited Nov. 20, 2020); *Phalanx Weapon System*, RAYTHEON MISSILES AND DEFENSE, https://www.raytheonmissilesanddefense.com/capabilities/products/phalanx-close-in-weapon-system (last visited Nov. 20, 2020).

article, the key aspect of autonomy is that a weapon system can select and attack targets without human intervention. Part III analyzes the argument that human judgment is required for selecting and attacking targets and contrasts that position against the current practice of States and their statements on the issue. Further, this Part looks specifically at the requirement to take precautions, as codified in Article 57 of AP I. Part IV concludes finding that no requirement for human judgment in selecting and attacking targets currently exists.

II. AUTONOMY

Autonomy, in particular the use of autonomy in weapons systems, is a major point of discussion between States. As Masahiro Kurosaki writes, "[A]utonomy in unmanned systems will be critical to future conflicts that will be fought and won with technology."[3] Many of these unmanned systems will be either assisted by or based almost completely on cyber capabilities.

Within the last ten years, formal discussions on autonomous weapons, or weapons that rely on autonomous functions such as machine learning or artificial intelligence, have failed to produce a common understanding of what "autonomy" even means.[4] As Chris Jenks notes, "the international community cannot even agree about what they disagree about."[5]

To some degree, the position individuals or States take on autonomous weapons may be influenced by the definitional decision on autonomy. For example, the International Committee of the Red Cross (ICRC) defines autonomous weapon systems as "weapon systems with autonomy in their 'critical functions' of selecting and attacking targets."[6] Further, the organization

3. Masahiro Kurosaki, *Towards the Special Computer Law of Targeting: 'Fully Autonomous' Weapons Systems and the Proportionality Test*, *in* NECESSITY AND PROPORTIONALITY IN INTERNATIONAL PEACE AND SECURITY LAW (Claus Kreß & Robert Lawless eds., forthcoming 2020).

4. Chris Jenks, *False Rubicons, Moral Panic, and Conceptual Cul-De-Sacs: Critiquing & Reframing the Call to Ban Lethal Autonomous Weapons*, 44 PEPPERDINE LAW REVIEW 1, 13 (2016).

5. *Id.*; *see also* Heather M. Roff & Richard Moyes, *Meaningful Human Control, Artificial Intelligence and Autonomous Weapons: Briefing Paper for Delegates at the Convention on Certain Conventional Weapons (CCW) Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS)),* at 1, 2016, http://www.article36.org/wp-content/uploads/2016/04/MHC-AI-and-AWS-FINAL.pdf.

6. INTERNATIONAL COMMITTEE OF THE RED CROSS, ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN ARMED CONFLICT: A HUMAN-CENTRED APPROACH 1, 2 (2019), https://www.icrc.org/en/download/file/96992/ai_and_machine_learning_in_armed_conflict-icrc.pdf [hereinafter ICRC, ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING].

takes the approach that such systems "are an immediate concern from a humanitarian, legal and ethical perspective, given the risk of loss of human control over weapons and the use of force."[7]

By contrast, the United Kingdom approaches autonomy more broadly, stating, "[f]ocusing solely on specific – or 'critical' – functions or activity in the lifecycle of a weapon is unlikely to be sufficient to ensure there is human control."[8] The United Kingdom argues that basing regulation on the characterization of a system's function is unhelpful. Instead, it asserts that "it is the cumulative effect of multiple safeguards across the development and operational lifecycle that establish human control of weapon systems. Therefore, human control should be considered and exercised throughout this lifecycle and in a way that is appropriate to the operational context."[9]

Such disparate views cause legal experts like Chris Jenks and Rain Liivoja to conclude that "autonomy is better thought of across several different spectrums."[10] They further add that "attempts at overall system categorization based on only one of the spectrums—machine complexity—lack practical utility."[11]

For the purposes of this article, a weapon system is autonomous "when it possesses both an intent (an encoded representation of a goal, a purpose, or a task to be completed) and the ability to act within its environment in furtherance of that goal."[12] Under this definition, autonomous weapons systems, including autonomous cyber capabilities, could be subject to human control, but also may function without constant, or even decisive, human control, including during the processes of selecting and engaging targets.

---

7. *Id.*

8. U.K. Mission Geneva, Convention on Certain Conventional Weapons Group of Government Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Agenda Item 5(d): Further Consideration of the Human Element in the Use of Lethal Force; Aspects of Human-Machine Interaction in the Development, Deployment and Use of Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, at 1, Mar. 25–29, 2019, https://www.unog.ch/80256EDD006B8954/(httpAssets)/85A4AA89AFCFD316C12583D3003EAB3E/$file/20190318-5(d)_HMI_Statement.pdf [hereinafter U.K. Statement].

9. *Id.* at 2.

10. Chris Jenks & Rain Liivoja, *Machine Autonomy and the Constant Care Obligation*, HUMANITARIAN LAW AND POLICY (Dec. 11, 2018), https://blogs.icrc.org/law-and-policy/2018/12/11/machine-autonomy-constant-care-obligation/.

11. *Id.*

12. TIM MCFARLAND, THE CONCEPT OF AUTONOMY' IN AUTONOMOUS CYBER CAPABILITIES UNDER INTERNATIONAL LAW (Rain Liivoja & Ann Väljataga eds., forthcoming 2021).

Weapons and weapons systems that are autonomous in this sense have raised the ire of many nongovernmental organizations (NGOs) and the ICRC, and have become the basis for much of the debate among States—particularly in the meetings of States Party to the CCW. Some scholars have argued that the CCW is the perfect forum to hear these debates and to regulate autonomous weapons.[13] Part III will analyze these discussions.

One additional definitional caveat is important. The consideration here of autonomous weapons systems is distinct from the question of weapons that may in the future utilize artificial intelligence. Artificial intelligence includes cognition.[14] While an autonomous weapons system does not necessarily require cognition to "learn" on the battlefield, this article considers weapons systems that use artificial intelligence or machine learning to adjust decision-making processes, but not weapons systems that are cognitive.

---

13. Qiang Li & Dan Xie, *Legal Regulation of AI Weapons under International Humanitarian Law: A Chinese Perspective*, HUMANITARIAN LAW AND POLICY (May 2, 2019), https://blogs.icrc.org/law-and-policy/2019/05/02/ai-weapon-ihl-legal-regulation-chinese-perspective/. Li and Xie argue:

> Moreover, the targeting of AI weapon systems is closely tied to their design and programming. The more autonomy they have, the higher the design and programming standards must be in order to meet the IHL requirements. For this purpose, the international community is encouraged to adopt a new convention specific to AI weapons, such as the Convention on Conventional Weapons and its Protocols, or the Convention against Anti-personnel Mines and Convention on Cluster Munitions.

14. As Dustin Lewis writes:

> AI science pertains in part to the development of computationally based understandings of intelligent behavior, typically through two interrelated steps. One of those steps concerns the determination of cognitive structures and processes and the corresponding design of ways to represent and reason effectively. The other step relates to the development of theories, models, data, equations, algorithms and/or systems that embody that understanding. So defined, AI systems are typically conceived as incorporating techniques—and leading to the development of tools—that enable systems to 'reason' more or less 'intelligently' and to 'act' more or less 'autonomously'. The systems might do so by, for example, interpreting natural languages and visual scenes; 'learning' (or, perhaps more commonly, training); drawing inferences; and making 'decisions' and taking action on those 'decisions'. The techniques and tools might be rooted in one or more of the following methods: those rooted in *logical reasoning* broadly conceived, which are sometimes also referred to as 'symbolic AI' (as a form of model-based methods); those rooted in *probability* (also as a form of model-based methods); and/or those rooted in *statistical reasoning and data* (as a form of data-dependent or data-driven methods).

Dustin A. Lewis, *Legal Reviews of Weapons, Means and Methods of Warfare Involving Artificial Intelligence: 16 Elements to Consider*, HUMANITARIAN LAW AND POLICY (Mar. 21, 2019), https://blogs.icrc.org/law-and-policy/2019/03/21/legal-reviews-weapons-means-methods-warfare-artificial-intelligence-16-elements-consider/.

III. HUMAN JUDGMENT AND PRECAUTIONS

I argue more in-depth elsewhere that the LOAC does not require weapons that utilize machine learning or artificial intelligence to be limited by some inclusion of human judgment in the processes of selecting and engaging targets.[15] I will briefly restate various views on this question to facilitate a discussion of how weapons that use machine learning and artificial intelligence, including cyber weapons, might be governed by the LOAC, including the rules on precautions.

Initially, it is important to confirm that the LOAC applies to the use of emerging technologies in general and to autonomous weapons systems or weapons that use machine learning and artificial intelligence in particular. This view is shared both by States[16] and by NGOs.[17] However, great debate exists as to how those weapons systems might comply with the LOAC.

In the past decade, various organizations have argued that any use of autonomous weapons would be unlawful because of the non-human element

---

15. Eric Talbot Jensen, *The (Erroneous) Requirement for Human Judgment (and Error) in the Law of Armed Conflict*, 96 INTERNATIONAL LAW STUDIES 26 (2020).

16. *See, e.g.*, Brazil, GGE on LAWS – 2019 1st Week, Challenges to IHL – Item 5(a), https://www.unog.ch/80256EDD006B8954/(httpAssets)/122DF2DAEE334DDBC12583CC003EFD6F/$file/Brazil+GGE+LAWS+2019+-+Item+5+a+-+IHL.pdf; Kingdom of the Netherlands, Statement of the Netherlands Delivered by Mr. Reint Vogelaar, First Secretary, Permanent Representation of the Kingdom of the Netherlands to the Conference on Disarmament at Group of Experts on LAWS, Agenda Item 5(a): An Exploration of the Potential Challenges Posed by Emerging Technologies in the Area of Lethal Autonomous Weapons Systems to International Humanitarian Law, Apr. 26, 2019, https://www.unog.ch/80256EDD006B8954/(httpAssets)/A2E0497EE93C232AC12583CB0037813B/$file/5a+NL+Statement+Legal+Challenges-final.pdf; Poland, 4th GGE on LAWS, Statement of the Delegation of Poland: General Comments, Mar. 25, 2019, https://www.unog.ch/80256EDD006B8954/(httpAssets)/5CAD5A1367E305A5C12583CC004CA205/$file/1.+GGE_LAWS_March+2019_PL+Statement_General+comments_25.03.2019.pdf; European Union, EU Statement, Group of Governmental Experts, Lethal Autonomous Weapons Systems, Convention on Certain Conventional Weapons, Mar. 25–29, 2019, https://www.unog.ch/80256EDD006B8954/(httpAssets)/EA84B3C2340F877DC12583CB003727F3/$file/ALIGNED+-+LAWS+GGE+EU+statement+IHL.pdf.

17. *See*, *e.g.*, Netta Goussac, *Safety Net or Tangled Web: Legal Reviews of AI in Weapons and War-Fighting*, HUMANITARIAN LAW AND POLICY (Apr. 18, 2019), https://blogs.icrc.org/law-and-policy/2019/04/18/safety-net-tangled-web-legal-reviews-ai-weapons-war-fighting (stating that "all weapons used in war must be used, and be capable of being used, in compliance with IHL" and that "each State that develops or acquires weapons that utilize AI must be satisfied that these weapons can be used in compliance with existing rules of warfare."); *see also* CAMPAIGN TO STOP KILLER ROBOTS, https://www.stopkillerrobots.org (last visited Nov. 20, 2020).

and have called for a ban on research and development of these weapons.[18] The ICRC, while acknowledging the key role of States in this discussion,[19] takes the following view:

> These rules require context-specific judgements to be taken by those who plan, decide upon and carry out attacks to ensure: distinction – between military objectives, which may law-fully be attacked, and civilians or civilian objects, which must not be attacked; proportionality – in terms of ensuring that the incidental civilian harm expected from an attack will not be excessive in relation to the concrete and direct military advantage anticipated; and to enable precautions in attack – so that risks to civilians can be further minimized.
>
> Where AI systems are used in attacks – whether as part of physical or cyber-weapon systems, or in decision-support systems – their design and use must enable combatants to make these judgements.[20]

In response to this argument, Masahiro Kurosaki counters that "[T]he existing human-centered paradigm is merely a product of the history of LOAC and does not exist a priori, an alternative approach to adjust to changing times, should be explored."[21]

States have taken widely disparate views on these questions. For example, in response to the call for a ban on autonomous weapons systems, the United Kingdom argues:

> [I]n the absence of any clearly articulated empirical evidence as to why existing regulation—including IHL—is inadequate to control developments in emerging technologies, the issue may well lie not with the processes themselves, but with the perceived ability of machines to assimilate, understand and meet the relevant extant legal and ethical standards.[22]

---

18. *See*, *e.g.*, CAMPAIGN TO STOP KILLER ROBOTS, *supra* note 17.
19. ICRC, ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING, *supra* note 6, at 2.
20. *Id.* at 7–8.
21. Kurosaki, *supra* note 3.
22. U.K. Statement, *supra* note 8. The United Kingdom also asserts:
> [W]eapons systems that cannot meet these standards will remain incapable of legal use as set out in existing national and international normative frameworks and will not be developed, fielded and used. All states should look to ensure they meet the basic obligations already set out in the relevant articles of IHL before pressing for bespoke legislation for as-yet undefined capabilities.

UK Mission Geneva, Statement regarding Agenda Item 5(a) at Meeting of Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons

Greece[23] and Germany[24] support the view that the LOAC requires a degree of human control in selecting and engaging targets, but as Rebecca Crootof notes there is little clarity on the specifics of that control.[25] As an example of the differing views on how human control might manifest in an autonomous weapon system, the United Kingdom states:

> [D]irect human involvement in every detailed action of a system or platform may not be practical or desirable under all circumstances. Instead a human-centred approach to autonomous technologies must take into account the operational context as well as the capabilities and limitations of the personnel deploying the weapon system.[26]

This operational context might include considerations such as whether the system is a land, air or sea-based system and the specific circumstances of both the development and the deployment of the system.[27]

Systems 3, Mar. 25–29, 2019, https://www.unog.ch/80256EDD006B8954/(httpAssets)/1ED3972D40AE53B5C12583D3003F8E5E/$file/20190318-5(a)_IHL_Statement.pdf.

23. Permanent Mission of Greece to the United Nations and the Other International Organizations Geneva, Statement by Greece, Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS), Potential Challenges Posed by Emerging Technologies in the Area of Lethal Autonomous Weapons Systems to International Humanitarian Law, at 1, Mar. 25–29, 2019, https://www.unog.ch/80256EDD006B8954/(http Assets)/D1B935800DF5F04DC12583CC002F3DD1/$file/GGE+LAWS+STATEMENT+by+GREECE-+Challenges+to+IHL.pdf.

24. Foreign Office, Federal Republic of Germany, Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems of 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, Statement by Germany – On Agenda Item 5(b) Further Consideration of the Human Element in the Use of Lethal Force; Aspects of Human Machine Interaction in the Development, Deployment and Use of Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Mar. 26, 2019, https://www.unog.ch/80256EDD006B8954/(http Assets)/2B8E772610C0F552C12583CB003A4192/$file/20190326+Statement3+Germany+GGE+LAWS.pdf.

25. Rebecca Crootof, *A Meaningful Floor for "Meaningful Human Control,"* 30 TEMPLE INTERNATIONAL AND COMPARATIVE LAW JOURNAL 53, 54 (2016).

26. U.K. Statement, *supra* note 8.

27. *Id.*

In 2019, U.S. Department of Defense General Counsel Paul Ney argued that autonomy makes and will continue to make weapons systems more accurate, more precise, and able to perform much more quickly.[28] In perhaps the strongest statement against the fixation on human control, Ney stated:

> In the U.S. perspective, there is nothing intrinsically valuable about manually operating a weapon system as opposed to operating it with an autonomous function. For example, existing law of war treaties do not seek to enhance "human control" as such. Rather, these treaties seek, among other things, to ensure the use of weapons consistent with the fundamental principles of distinction and proportionality, and with the obligation to take feasible precautions for the protection of the civilian population. Although "human control" can be a useful means in implementing these principles, "human control" as such is not, and should not be, an end in itself. In our view, we should not be developing novel principles that stigmatize the use of emerging technologies, when these technologies could significantly enhance how the existing principles of the law of war are implemented in military operations.[29]

Two points appear clear from this brief review of State perspectives. First, all autonomous weapons systems developed and employed must comply with the LOAC. Second, there is no consensus as to the degree of human control necessary to comply with the LOAC.

Echoing Ney's statement above, the focus of international regulation should be on LOAC compliance, and not on who or what is bringing about that compliance. As I conclude elsewhere:

> [T]he legal standard for weapon systems using machine learning and artificial intelligence should be the "best application possible" rather than the "best application humanly possible." International focus on the decisions

---

28. *See* Paul C. Ney Jr., General Counsel, U.S. Department of Defense, Keynote Address at the Israel Defense Forces 3rd International Conference on the Law of Armed Conflict (May 28, 2019), https://www.lawfareblog.com/defense-department-general-counsel-remarks-idf-conference [hereinafter Ney Address].

29. *Id.* For additional statements by the United States in the context of the CCW discussions, see Group of Government Experts of the High Contracting Parties 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, Human-Machine Interaction in the Development, Deployment and Use of Emerging Technologies in the Area of Lethal Autonomous Weapons Systems 2 (2018), U.N. Doc. CCW/GGE.2/2018/WP.4 (2018).

> of warfare, rather than the decisionmakers, will benefit all concerned and result in greater protections for the participants in and the victims of armed conflict.[30]

With that foundation, a more specific analysis of precautions in attack, as codified in Article 57 of AP I, is in order to determine key focus areas in ensuring compliance with the LOAC—particularly by militaries that develop and employ autonomous systems to select and engage targets.

A. Article 57(1) – "Constant Care"

Although Article 57(1) falls under the heading of "Precautions in Attack," its broad coverage includes the conduct of "military operations" generally.[31] The obligation on States is one of "constant care."[32] Autonomous systems have already been created to take an active role in non-combat military operations (for example, logistics).[33] Although this article focuses on the use of autonomy in combat situations, non-combat autonomous systems can also cause death or injury and therefore deserve some comment here.

Jenks and Liivoja address the issue of autonomy with non-combat vehicles. They argue:

> Article 57(1) would require that autonomous vehicles be designed and relied upon with the safety of the civilian population in mind. Thus, an autonomous ground vehicle should avoid, for example, injuring civilians or damaging civilian building[s] and infrastructure. Likewise, an autonomous aerial vehicle should be capable of avoiding civilian air traffic and not crash

30. Jensen, *supra* note 15, at 57.

31. The *Commentary* to AP I states: "The term 'military operations' should be understood to mean any movements, manoeuvres and other activities whatsoever carried out by the armed forces with a view to combat." COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 ¶ 2191 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987) [hereinafter COMMENTARY ON THE ADDITIONAL PROTOCOLS].

32. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts art. 57(1), June 8, 1977, 1125 U.N.T.S 3 [hereinafter AP I] ("In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects.").

33. Jon Harper, *Autonomous Helicopters Seen as Wave of the Future*, NATIONAL DEFENSE MAGAZINE (Feb. 2, 2018), https://www.nationaldefensemagazine.org/articles/2018/2/20/autonomous-helicopters-seen-as-wave-of-the-future.

> into and damage civilian objects upon a failure of the communication link to its operator.[34]

This quote highlights the fact that non-combat autonomous systems may still lead to death or injury and thus commanders need to employ them with constant care for the civilian population.

The constant care obligation applies equally to autonomous cyber operations. As I write elsewhere, "commanders and all persons conducting cyber operations must recognize and accept the legal obligation to exercise constant care in all military operations, including cyber operations."[35]

The *Tallinn Manual 2.0* also takes this position, stating, "During hostilities involving cyber operations, constant care shall be taken to spare the civilian population, individual civilians, and civilian objects."[36] The Group of Experts was unanimous in the formulation of this rule and argued:

> Use of the word 'constant' denotes that the duty to take care to protect civilians and civilian objects is of a continuing nature throughout cyber operations; all those involved in the operation must discharge the duty. The law admits of no situation in which, or time when, individuals involved in the planning and execution process may ignore the effects of their operations on civilians or civilian objects. In the cyber context, this requires situational awareness at all times, not merely during the preparatory stage of an operation.[37]

The "constant" nature of this requirement applies equally to autonomous cyber systems. In designing and utilizing such systems, even outside the context of an attack, military operators must ensure that the autonomous system can exercise constant care.

---

34. Jenks & Liivoja, *supra* note 10.

35. Eric Talbot Jensen, *Cyber Attacks: Proportionality and Precautions in Attack*, 89 INTERNATIONAL LAW STUDIES 198, 204 (2013).

36. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE r. 114, at 476 (Michael N. Schmitt ed., 2017) [hereinafter TALLINN MANUAL 2.0]. Note that the author was a member of the Group of Experts for both *Tallinn Manual on the International Law Applicable to Cyber Warfare* (2013) and *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.

37. *Id.* at 477 (citations omitted).

B. Article 57(2) – "Precautions in Attack"

Article 57(2) codifies the current customary law on applying "precautions in attack." These provisions are among those recognized as binding on all States that desire to utilize weapons—whether autonomous or not. The question raised by autonomous weapons systems is whether these systems can comply with the requirements stated in Article 57. Professor Suresh Venkatasubramanian perhaps best describes this question:

> If we look at the principles of distinction, proportionality and precautions under international humanitarian law as guidance for when an attack is considered permissible, we see a lot of judgement framed in terms that to a computer scientist seem imprecise. One might argue that the vagueness in these terms is by design: it allows for nuance and context as well as human expert judgement to play in a role in a decision, much like how the discretion of a judge plays a role in judging the severity of a sentence. Another view of this 'vagueness by design' is that it allows for future *contestability*: if commanders are forced to defend a decision later on, they can do so by appealing to their own experience and judgement in interpreting a situation. . . . But what of algorithm-driven targeting? How is a system supposed to learn what targets satisfy principles of proportionality, distinction and precaution when to do so it must rely on a precise labeling that almost cannot exist by design.[38]

Accordingly, this section will analyze the legal requirements contained in the subsections of Article 57(2) and (3) and argue that despite potential technological and conceptual limitations, none of those subsections present an insurmountable legal obstacle to the use of autonomous weapons systems.

1. "Those Who Plan or Decide upon an Attack"

Beginning with Article 57(2), the first provision bearing on the use of autonomous weapons systems, including weapons with autonomous cyber capability, is subparagraph (a). That subparagraph specifically regulates those who plan or decide upon an attack. The ICRC takes the following view:

38. Suresh Venkatasubramanian, *Structural Disconnects between Algorithmic Decision-Making and the Law*, HUMANITARIAN LAW AND POLICY (Apr. 25, 2019), https://blogs.icrc.org/law-and-policy/2019/04/25/structural-disconnects-algorithmic-decision-making-law/.

> International humanitarian law (IHL) requires that those who plan, decide upon and carry out attacks make certain judgements in applying the norms when launching an attack. Ethical considerations parallel this requirement – demanding that human agency and intention be retained in decisions to use force.[39]

Although it is not clear from the text of this provision that human judgment is required, the ICRC argues that both legal and ethical considerations require human judgment. Others take the same approach, arguing specifically that this provision establishes an accountability mechanism that precludes autonomous systems. For example, Roff and Moyes describe accountability as follows:

> [A]n ex post process to locate responsibility or liability with human agents, . . . [that] also establishes a framework of expectation that can guide human agents to align their behavior with expected and appropriate standards. Standards for accountability, moreover, need to ensure that responsibility and liability will be apportioned equitably, and that sanctions will be applied that are commensurate with the wrongdoing (whether intentional or inadvertent) and with the severity of harm that may have been caused.[40]

As inferred above, some complain that autonomous weapons systems that select and engage targets leave no method of accountability for decisions that violate the LOAC. Others counter that accountability is not, and has not been, focused solely on the person pulling the trigger, which, in the case of

---

39. International Committee of the Red Cross, Statement of the International Committee of the Red Cross (ICRC), Convention on Certain Conventional Weapons (CCW), Group of Governmental Experts on Lethal Autonomous Weapons Systems, Apr. 9–13, 2018, https://www.unog.ch/80256EDD006B8954/(httpAssets)/B718A7D561773A68C12583BB003AF8A5/$file/CCW+GGE+April+2018+-+ICRC+general+debate.pdf. The ICRC also asserts:

> [E]thical considerations very much parallel the requirement for a minimum level of human control over weapon systems and the use of force . . . . From an ethical viewpoint, "meaningful", "effective" or "appropriate" human control would be the type and degree of control that preserves human agency and upholds moral responsibility in decisions to use force. This . . . requires a sufficiently direct and close connection to be maintained between the human intent of the user and the eventual consequences of the operation of the weapon system in a specific attack.

INTERNATIONAL COMMITTEE OF THE RED CROSS, ETHICS AND AUTONOMOUS WEAPONS SYSTEMS: AN ETHICAL BASIS FOR HUMAN CONTROL? 22 (2018), https://www.icrc.org/en/download/file/69961/icrc_ethics_and_autonomous_weapon_systems_report_3_april_2018.pdf.

40. Roff & Moyes, *supra* note 5, at 3.

autonomous weapons systems, would mean the system itself.[41] The language of those who "plan or decide" is obviously meant to include not just the trigger puller, but also those at all levels of command and decisionmaking. This would include, in particular, those who order autonomous weapons systems into battle. As shown below, the *Commentary* and the statements of the delegations to the negotiating conference that led to AP I confirm this understanding.

The phrase "plan or decide" was a topic of discussion at the AP I negotiating conference. As the 1987 *Commentary on the Additional Protocols* states:

> The terminology used in this provision led to some criticism and explanatory statements. Some considered that the introductory words ("those who plan or decide upon an attack") could lay a heavy burden of responsibility on subordinate officers who are not always capable of taking such decisions, which should really fall upon higher ranking officers. This view is not without grounds, but it is clear that a very large majority of delegations at the Diplomatic Conference wished to cover all situations with a single provision, including those which may arise during close combat where commanding officers, even those of subordinate rank, may have to take very serious decisions regarding the fate of the civilian population and civilian objects. It clearly follows that the high command of an army has the duty to instruct personnel adequately so that the latter, even if of low rank, can act correctly in the situations envisaged.[42]

Many statements made by the delegations at the conference support this view. For example, the Swiss delegation stated that it "was critical of paragraphs 2 and 3 of Article 50 because they lacked clarity; particularly the words 'Those who plan or decide upon an attack . . . ' in paragraph 2 (a)."[43] Others,

---

41. *See*, *e.g.*, Merel Ekelhof, *Autonomous Weapons: Operationalizing Meaningful Human Control*, HUMANITARIAN LAW AND POLICY (Aug. 15, 2018), https://blogs.icrc.org/law-and-policy/2018/08/15/autonomous-weapons-operationalizing-meaningful-human-control/.

42. COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 31, ¶ 2197.

43. 6 OFFICIAL RECORDS OF THE DIPLOMATIC CONFERENCE ON THE REAFFIRMATION AND DEVELOPMENT OF INTERNATIONAL HUMANITARIAN LAW APPLICABLE IN ARMED CONFLICTS 212, ¶ 43 (1978). Further, the delegation concluded,

> That ambiguous wording might well place a burden or responsibility on junior military personnel which ought normally to be borne by those of higher rank. The obligations set out in Article 50 could concern the high commands only - the higher grades of the military hierarchy, and it was thus that Switzerland would interpret that provision.

Id.

including delegations from Afghanistan,[44] Austria,[45] the Netherlands,[46] and Sweden[47] echoed this statement.

Contemporary commentators express the same concerns. For example, Rebecca Crootof, in speaking about the command levels at which human control should be exercised, writes:

> [T]here is still no agreement as to the level of decision-making at which human control must occur. The commander determining the rules of engagement is exercising a certain kind of control, the commander ordering a particular attack is exercising another, and the individual implementing that order might exercise yet another kind of control.
>
> Given the difficulty in pinning down what "meaningful human control" actually requires, "[s]everal states [have] expressed skepticism over the added value of the suggested concept, assessing it as being too vague, subjective and unclear."[48]

Moreover, Roff and Moyes argue:

> At its most basic level, the requirement for [meaningful human control] develops from two premises: 1. That a machine applying force and operating without any human control whatsoever is broadly considered unacceptable. 2. That a human simply pressing a 'fire' button in response to indications from a computer, without cognitive clarity or awareness, is not sufficient to be considered 'human control' in a substantive sense.[49]

In responding to the second point raised by Roff and Moyes, Merel Ekelhof poses an interesting scenario in which a fighter pilot is sent on an attack mission to deliver ordnance on an enemy position. As is normal in military operations, a targeting cell, which includes a lawyer, reviewed the target prior to its approval. The pilot is then assigned the mission, briefed on the intelligence situation, and given specific details about the target—all of which is also loaded into the aircraft's targeting systems. In this particular example, poor weather prevents the pilot from having good visibility of the target.

---

44. *Id.* at 219.
45. *Id.* at 212, ¶ 46.
46. *Id.* at 205, ¶ 1.
47. *Id.* at 236–37.
48. Crootof, *supra* note 25, at 58 (citations omitted).
49. Roff & Moyes, *supra* note 5, at 1 (citation omitted).

Ekelhof argues that in such circumstances, the pilot will have to "rely on the aircraft's systems, the weapons guidance systems, and the validation procedure at the operational level to ensure s/he is striking a legitimate military objective in a lawful manner."[50] Accordingly, she continues:

> Thus, the information about the lawfulness of the action largely depends on the operator's trust in his or her superiors in the chain of command (to provide proper briefing materials and conduct target validation during the planning phase), the F-16 board computer (suggesting the appropriate time for weapon's release) and the weapon's guidance system (navigating the munitions to the target). At no point during our F2T2EA process will the pilot gather intelligence about the target or conduct legal analyses.[51]

Ekelhof's scenario aptly illustrates the point that the deliverer of the ordnance—the individual attacking—is doing so having neither seen the target, nor verified the intelligence. Such attacks take place all the time in modern warfare. Similar scenarios can be described with respect to artillery and most "beyond the line of sight" weapons.

After analyzing this common scenario, Ekelhof concludes:

> the concept of meaningful human control is not the only, or perhaps the most fitting, approach to analyzing (the effect of autonomous technologies on) human control over critical targeting decisions. Instead, the more appropriate analytical lens would be one that recognizes the distributed nature of control in military decision-making in order to pay due regard to a practice that has shaped operations over the past decades and continues to be standard in contemporary targeting.[52]

Ekelhof's scenario and her conclusions highlight the importance of the language in Article 57, which places responsibility for ensuring precautions not only with the "trigger puller," but also with many others in the military decision-making process. This would, of course, also apply to commanders who employ autonomous weapons systems, including cyber systems.

Arguing that autonomous weapons systems cannot be utilized in conformity with the LOAC because they lack an accountability mechanism is an overly narrow reading of the words in Article 57. The responsibility falls not only to those who execute the attacks (including an autonomous weapons

50. Ekelhof, *supra* note 41.
51. *Id.*
52. *Id.*

system), but also to those in "higher commands" such as the local, operational, and strategic military commanders who will employ those weapons systems on the battlefield, and those in the research, production, review, and approval processes. A more holistic understanding of "those who plan or decide upon an attack" leaves no accountability gap.

This analysis applies equally to weapons utilizing autonomous cyber capabilities. In the commentary discussing Rule 115,[53] *Tallinn Manual 2.0* states:

> An important feature of Rule 115 is its focus on planners and decision-makers. Those who execute cyber attacks may sometimes also be the ones who approve them. In the case of certain attacks, the individual actually executing the attack has the capability to determine the nature of the target and to cancel the operation . . . On other occasions, the person executing the attack may not be privy to information as to its character or even the identity of the target. He or she may simply be carrying out instructions to deliver the cyber weapon against a predetermined part of the cyber infrastructure. Under these circumstances, the duty of the individual carrying out the cyber attack to verify would be limited to those measures that are feasible in the circumstances.[54]

Because of the technology required for cyber attacks, a combination of individuals likely designed and built the cyber tool, determined the accessibility of the target, mapped the "surrounding" cyber network, installed the malware, and executed the malware. Consider also the additional leaders and commanders at the tactical, operational, and strategic level who are not cyber experts but will make significant decisions concerning the employment of cyber tools in their area of operations. To the extent that they "plan or decide upon" the attack, they all have the legal obligation to comply with this precaution. Despite this potentially expanded field of players in a cyber attack, there is nothing inherent in the technology that would prevent a full and thorough analysis under Article 57. As *Tallinn Manual 2.0* states:

> The limitation of this Rule to those who plan or decide upon cyber attacks should not be interpreted as relieving others of the obligation to take appropriate steps should information come to their attention that suggests an

53. Rule 115 states: "Those who plan or decide upon a cyber attack shall do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection." TALLINN MANUAL 2.0, *supra* note 36, at 478.

54. *Id.* (citation omitted).

> intended target of a cyber attack is a protected person or object, or that the attack would otherwise be prohibited.[55]

One last comment on this point is important before moving on to further provisions of Article 57. In a recent publication, Laura Dickinson argues that administrative accountability can also play a key role in the lawful use of cyber capabilities during military operations.[56] Dickinson contends that discussions about the potential of administrative accountability to regulate and ensure the compliance of cyber operations with the LOAC have been largely absent. She asserts:

> Such accountability includes multiple administrative procedures, inquiries, sanctions, and reforms that can be deployed within the military or the administrative state more broadly to respond to an incident in which a violation of IHL/LOAC may have occurred. This form of accountability may be particularly useful in the case of LAWS, because the restrictions of criminal law, such as the intent requirement for most crimes, may not apply in many circumstances. Administrative accountability is flexible both in the process by which it unfolds and in the remedies available, offering the prospect of both individual sanctions as well as broader organizational reforms.[57]

Dickinson's argument for including administrative accountability in the review process further supports an expansive view of accountability. Too narrow a view on accountability unnecessarily limits the application of legal norms to autonomy on the battlefield.

2. "Do Everything Feasible to Verify" – Distinction

Article 57(2)(a)(i) effectively restates the LOAC principle of distinction and requires those who plan or decide upon attacks to do everything feasible to verify that the targets are appropriate military objectives. The content of this rule needs no explanation here. The important question for this discussion is whether autonomous weapons systems can apply the principle of distinction, and how that might be assured.

---

55. *Id.*

56. Laura A. Dickinson, *Lethal Autonomous Weapon Systems: The Overlooked Importance of Administrative Accountability*, *in* THE IMPACT OF EMERGING TECHNOLOGIES ON THE LAW OF ARMED CONFLICT 69–85 (Eric Talbot Jensen & Ronald Alcala eds., 2019).

57. *Id.* at 71.

Distinction is often believed to be a principle that requires human judgment and discretion because of the complexity of the decisions on the modern battlefield. Rather, meaningful adherence to distinction is both a technological question and a legal question. An analysis on whether autonomous weapons systems and those that utilize autonomous cyber capabilities are able to satisfactorily comply with the rules of distinction must be assessed through this latter framework. Moreover, whether or when technology will be capable of applying human judgment is beyond the scope of this paper, and not vital to the current discussion. Recent technological developments may allow the integration of biologically realistic neural networks with computer hardware in a way that could create an autonomous weapon with thinking and processing elements.[58] Such developments might significantly alter the discussion concerning the application of human judgment by weapons systems.

However, accepting that technology is, at present, incapable of human-like judgment, the question at hand is what legal obligation, if any, stipulates that an autonomous weapons system could not comply with distinction? Recall Ney's 2019 remarks, which stated:

> In the U.S. perspective, there is nothing intrinsically valuable about manually operating a weapon system as opposed to operating it with an autonomous function. For example, existing law of war treaties do not seek to enhance "human control" as such. Rather, these treaties seek, among other things, to ensure the use of weapons consistent with the fundamental principles of distinction and proportionality, and with the obligation to take feasible precautions for the protection of the civilian population. Although "human control" can be a useful means in implementing these principles, "human control" as such is not, and should not be, an end in itself.[59]

Other than the assertion that humans must be involved in any decision to select or engage targets—an assertion that has not been accepted by the international community as legally binding—there is no legal basis for arguing that autonomous systems cannot achieve compliance with the LOAC, including the principle of distinction.

---

58. Carolyn Sharp, Status of the Operator: Biologically Inspired Computing as Both a Weapon and an Effector of Laws of War Compliance (on file with author).

59. Ney Address, *supra* note 28.

With respect to cyber operations, cyber actors have used both indiscriminate[60] and very carefully tailored[61] tools in conducting cyber operations. As with all autonomous weapons systems, autonomous cyber tools would have to be able to apply force discriminately.

States that develop autonomous systems do not abrogate their legal duty to ensure that every weapons system employed by its armed forces complies with the LOAC. While not always strictly observed,[62] States comply with this requirement through a weapons review process[63] that has been well documented and discussed. This weapons review process includes an initial review as well as any necessary follow-up reviews for weapons systems that might change, adapt, or "learn" on the battlefield.[64] States can neither develop nor employ an autonomous weapon system, whether cyber or otherwise, that cannot apply precautions, including the principle of distinction.

3. "Take All Feasible Precautions in the Choice of Means and Methods" – Weaponeering

Article 57(2)(a)(ii) requires States to "take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects." Accordingly, the weapons and tactics armed forces utilize in armed conflict, including potential autonomous weapons

60. Statement from the Press Secretary, WHITE HOUSE (Feb. 15, 2018), https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.

61. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, NEW YORK TIMES (June 1, 2012), https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

62. INTERNATIONAL COMMITTEE OF THE RED CROSS, A GUIDE TO THE LEGAL REVIEW OF NEW WEAPONS, MEANS AND METHODS OF WARFARE 5 (2006), https://e-brief.icrc.org/wp-content/uploads/2016/09/12-A-Guide-to-the-Legal-Review-of-New-Weapons.pdf.

63. AP I, *supra* note 32, art. 36; U.S. Department of Defense, Directive 5000.01, The Defense Acquisition System ¶ 1.2.v. (2003) (Incorporating Change 2, Aug. 31, 2018), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/500001p.pdf; OFFICE OF THE GENERAL COUNSEL, U.S. DEPARTMENT OF DEFENSE, LAW OF WAR MANUAL § 6.2 (rev. ed., Dec. 2016).

64. *See* U.S. Department of Defense, Directive 3000.09, Autonomy in Weapon Systems ¶ 4.c. (2012) (Incorporating Change 1, May 8, 2017) (requiring certain autonomous and semi-autonomous weapons to be considered for approval in accordance with DoD Directive 5000.01).

systems and those that utilize artificial intelligence or machine learning, must be capable of complying with this rule.

Although this is a significant and necessarily burdensome requirement clearly affecting the research, development, and employment of weapons and tactics, it is important to note that these provisions equally apply to autonomous weapons systems, including autonomous cyber weapons. As Rain Liivoja points out, most LOAC rules are "technology-neutral" or "technology-indifferent," meaning that they need not change with every new technological development.[65] Echoing Liivoja, Marco Longobardo states:

> [T]he rules on the protection of civilians are the same regardless of whether hostilities are conducted with swords, bows, muskets, bombers, drones, or robots; simply, civilians must not be made the object of attacks, period. In this sense, most international humanitarian law rules are 'technology-indifferent', that is, they govern 'the conduct of hostilities and offer[] protection to persons not taking part in hostilities [] all quite irrespective of the means and methods of warfare the belligerents adopt and other technology that they use.[66]

As Longobardo argues, this requirement is technology-neutral and therefore poses no additional limitation on the use of autonomous weapons systems, whether cyber or non-cyber. Any weapons review process must account for this provision of the law and must ensure that autonomous weapons are capable of applying this rule. No additional legal requirement exists.

4. "Refrain from Deciding to Launch an Attack" – Proportionality

Article 57(2)(a)(iii) is commonly known as the "proportionality rule." This provision is explicitly clear that applying the principle of proportionality (one of the general protections for civilians[67]) is a legal requirement for all those who plan or decide upon attacks.

---

65. Rain Liivoja, *Technological Change and the Evolution of the Law of War*, 97 INTERNATIONAL REVIEW OF THE RED CROSS 1157, 1168–69 (2016).

66. Marco Longobardo, *Training and Education of Armed Forces in the Age of High-Tech Hostilities*, *in* USE AND MISUSE OF NEW TECHNOLOGIES: CONTEMPORARY CHALLENGES IN INTERNATIONAL AND EUROPEAN LAW 73, 77 (Elena Carpanelli & Nicole Lazzerini eds., 2019).

67. AP I, *supra* 32, art. 51(5)(b).

Masahiro Kurosaki writes extensively on the application of proportionality to autonomous weapons systems. He argues that the principle of proportionality applies to autonomous weapons systems and would equally apply to "computer-centered" systems.[68]

> The principle of proportionality in modern LOAC has developed through the "reasonable military commander" standard. However, it is not intrinsically tied to, or at least not being limited to, the judgment of military commanders. It could be subject to adaptation in its application to a given circumstance by way of legal standards reflecting the sophisticated characteristics of fully AWS [autonomous weapons systems].[69]

As Kurosaki notes, there is no legal limitation on having an autonomous weapon system apply the principle of proportionality in selecting and engaging targets, assuming it could adequately apply the rule. In an interesting twist of argument, Kurosaki further asserts that the Martens Clause—a principle of law often used by opponents of autonomous weapons systems[70]—actually supports the use of autonomous weapons, particularly if it could limit the impacts on civilians.

> [I]t should be recalled that, as the Martens Clause enunciates, the humanitarian purpose of LOAC consists in protecting "the inhabitants and belligerents," no more and no less. The ICTY similarly opined that "[t]he basic obligation to spare civilians and civilian objects as much as possible must guide the attacking party when considering the proportionality of an attack."[71]

The content of the proportionality rule is not disputed with respect to autonomous weapons systems. Rather, the question is whether such systems can apply the rule. As mentioned above, it is unclear now what technological advancements might allow. What is clear is that any State intending to field an autonomous weapons system that selects and engages targets must meet the LOAC requirement of applying the rule of proportionality as part of the precautions in the attack.

---

68. Kurosaki, *supra* note 3.

69. *Id.*

70. Rob Sparrow, *Ethics as a Source of Law: The Martens Clause and Autonomous Weapons*, HUMANITARIAN LAW AND POLICY (Aug. 15, 2018), https://blogs.icrc.org/law-and-policy/2017/11/14/ethics-source-law-martens-clause-autonomous-weapons/.

71. Kurosaki, *supra* note 3.

In the context of the LOAC, cyber tools are rarely used and there is no public record of fully autonomous cyber tools being used. However, the principle of proportionality applies to both cyber tools utilized under the direct control of humans, as advocated in *Tallinn Manual 2.0*[72] and by others,[73] and to autonomous cyber capabilities.

5. "An Attack Shall Be Canceled or Suspended"

Article 57(2)(b) requires the attacker cancel or suspend a planned attack when the proportionality calculus changes such that the attack would violate the LOAC. Certainly, there are some attacks that, once triggered, cannot be canceled or suspended (for example, the launching of a missile or the shooting of a field cannon). Michael Horowitz and Paul Scharre write:

> [H]umans have been employing weapons where they lack perfect, real-time situational awareness of the target area since at least the invention of the catapult" and "the essence of a projectile weapon, since the first time a human hurled a rock in anger, is the inability to suspend and abort the attack after launch.[74]

Until the point that the attack is actually launched, the targeter must continue to apply the LOAC and cancel or suspend any attack that, due to a change in circumstances, becomes unlawful.

All autonomous weapons systems, including autonomous cyber systems, must have the capacity to cancel or suspend an attack based on either evidence provided externally or on evidence developed internally. *Tallinn Manual 2.0* illustrates this point with the following example:

> For example, assume that a cyber attack is planned and all preparations are completed, including mapping the network and determining the nature of the target system. The attackers are awaiting authorisation by the approving authority. Assume further that an operator is continuously monitoring the network. Any material changes in the cyber environment of the proposed target must be relayed to the commander and other relevant personnel as soon as possible.[75]

---

72. TALLINN MANUAL 2.0, *supra* note 36, r. 117, at 481.

73. Jensen, *supra* note 35, at 204–09.

74. MICHAEL C. HOROWITZ & PAUL SCHARRE, CENTER FOR A NEW AMERICAN SECURITY, MEANINGFUL HUMAN CONTROL IN WEAPON SYSTEMS: A PRIMER 7 (2015).

75. TALLINN MANUAL 2.0, *supra* note 36, r. 115, at 479.

This is at least in part a design requirement that would be reviewed and tested as part of the weapons review process. While a legal requirement with which States must comply, there is nothing inherent in the construction of autonomous weapons that would prevent them from complying with this rule.

C. Article 57(3) – "When a Choice Is Possible between Several Military Objectives"

The last provision of Article 57 that is likely to impact the deployment of autonomous weapons systems, including autonomous cyber systems, is Article 57(3), which states: "When a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects."[76]

Two aspects of this provision deserve consideration here. First, as this type of a decision would be one that inherently requires judgment, any autonomous weapon system would have to be capable of correctly making decisions that comply with law and policy. For autonomous weapons, assessing this capability would likely need to be a part of the weapons review process.

Second, the legal requirements of this provision strongly argue for the presence of autonomous weapons systems on the battlefield, and the use of autonomous systems more generally. As Ashley Deeks states:

> One reason for the military's attraction to AI is that it can help manage doubt. Every day, especially on the urban battlefield, militaries confront questions about what they are seeing: is that person holding a video camera or a rocket launcher? Why is there very little pedestrian traffic in the market today? Is the person I just detained likely to endanger our forces if released? Will a strike on that warehouse using a joint direct attack munition produce excessive collateral damage? Each of these questions requires decision-making in the face of uncertainty. AI tools can help categorize objects, identify anomalies, and make predictions up to a particular confidence level. These algorithms will be especially useful if they produce recommendations that are sensitive to the precise questions that LOAC requires militaries to answer.[77]

---

76. AP I, *supra* note 32, art. 57(3).

77. Ashley Deeks, *Coding the Law of Armed Conflict: First Steps*, *in* THE LAW OF ARMED CONFLICT IN 2040 (Matthew C. Waxman ed., forthcoming 2020).

Autonomous systems are systems that utilize ongoing machine learning and artificial intelligence. Therefore, the ability of such systems to accurately assess data concerning a wide variety of battlefield questions will continually increase. The interconnection of sensors, data processors, and algorithmic assessments will assuredly enhance the battlefield commander's ability to gather, assess, and exploit intelligence.

The same holds true when assisting commanders in surveying which targets are the least dangerous to civilians. Furthermore, the structural survivability of non-cyber autonomous systems[78] increases the ability to loiter and gather intelligence—thereby allowing for more comprehensive and thoughtful determinations about selecting and engaging targets. As Charles Trumbull states:

> Advances in robotics and AI will lead to weapons with far greater endurance than humans. . . . Machines "do not get tired, frightened, bored, or angry." They do not suffer the effects of post-traumatic stress disorder or seek revenge after witnessing their fellow soldiers killed in action. Accordingly, autonomous weapons are not susceptible to the human frailties that often lead to war crimes.[79]

To the extent that autonomous weapons live up to these expectations, they may prove to be a significant aid in complying with Article 57(3).

IV. CONCLUSION

As the analysis above indicates, the requirement to take precautions in attack does not present an unassailable legal impediment to the research, develop-

78. *See* ANDREW FEICKERT, JENNIFER K. ELSEA, LAWRENCE KAPP & LAURIE A. HARRIS, CONG. RESEARCH SERV., R45392, U.S. GROUND FORCES ROBOTICS AND AUTONOMOUS SYSTEMS (RAS) AND ARTIFICIAL INTELLIGENCE (AI): CONSIDERATIONS FOR CONGRESS 34 (2018) ("[P]roponents of such systems argue that human emotions—fear, anger, and the instinct for self-preservation—may lead to adverse consequences on the battlefield. Robots, they posit, may not be subject to human errors or unlawful behavior induced by human emotions.").

79. Charles P. Trumbull IV, *Autonomous Weapons: How Existing Law Can Regulate Future Weapons*, 34 EMORY INTERNATIONAL LAW REVIEW 533, 545–46 (2020) (citations omitted). *See also* Kurosaki, *supra* note 3 ("LOAC cannot go so far as to strictly demand human soldiers to protect civilians at the sacrifice of their own lives. Machines, however, may be exposed to the risk of destruction, hereby creating more opportunities for saving innocent civilians.").

ment, or employment of autonomous weapons systems, including autonomous cyber systems, provided such systems are subject to a rigorous weapons review. Furthermore, because Article 57 of Additional Protocol I applies, without prejudice, to all who plan or decide to attack, autonomous weapons remain within the confines of the LOAC requirements. Therefore, with rigorous weapons review processes in place that continually examine the autonomous system's continued "learning," and absent any legal preclusion to compliant systems, proposed autonomous weapons bans are unlikely to be successful—especially considering the present success of autonomous weapons already in use.