AUTONOMOUS WEAPON SYSTEMS UNDER INTERNATIONAL HUMANITARIAN LAW

A TRIPLE LENS APPROACH

Shahinaz Atlam

Assistant Professor of Public International Law
Faculty of Law
Ain Shams University

Abstract

Autonomous Weapon Systems (AWS) — also referred to as Lethal Autonomous Weapon Systems (LAWS) or "Killer Robots" — do not have a universally agreed-upon definition. Despite over a decade of discussions within the United Nations framework, states remain divided over their definition, legal nature, and the applicable legal frameworks. This division is echoed in academic and military literature. Some scholars support the development and use of such weapons, arguing that they outperform humans in complying with the principles of international humanitarian law. Conversely, others contend that, due to their non-human nature, these systems are inherently incapable of adhering to the fundamental principles of IHL, particularly proportionality and precaution, as these require cognitive assessments that only humans can perform and which, to date, cannot be transferred to machines.

In light of this division, the study examines the challenges posed by AWS within the framework of IHL, adopting a complementary three-dimensional approach: conceptual, legal, and technical-operational. The study is based on the premise that any accurate legal assessment of these weapons must be grounded in an understanding of their nature and the technologies that enable their autonomy. Accordingly, while the analysis focuses primarily on weapons law and targeting law, it also addresses the technical dimensions of these systems to show how autonomy is embedded in algorithms and computational processes, and what risks this entails from an IHL perspective.

This theoretical and technical analysis is complemented by examples of existing systems and supported by case studies — particularly Ukraine and Gaza — to examine how AWS are used in practice and the humanitarian consequences they produce.

The study concludes that, given the current state of technology, delegating decisions on the use of force — especially lethal force against human targets — to machines undermines existing legal frameworks and complicates legal accountability for unlawful attacks.

Keywords: Autonomous Weapon Systems (AWS), Artificial Intelligence (AI), Loitering Munitions, Weapons Law, Targeting Law, Autonomy in Warfare, Technology and Armed Conflict.

الملخص

أنظمة الأسلحة الذاتية — والتي يُشار إليها أيضًا باسم أنظمة الأسلحة الذاتية الفتاكة أو الروبوتات القاتلة — لا تتمتع بتعريف متفق عليه عالميًا. برغم مرور أكثر من عقد من المباحثات في إطار الأمم المتحدة، لا تزال الدول منقسمة حول تعريفها، طبيعتها القانونية، والأطر القانونية المنطبقة عليها. هذا الانقسام يجد صداه في الدراسات الأكاديمية والعسكرية التي أُجريت على هذه الأنظمة. فمن الفقه من يدعم تطوير واستخدام تلك الأسلحة زعمًا أنها أفضل من الإنسان في الامتثال لمبادئ القانون الدولي الإنساني، وفي المقابل جانب آخر يرى أنها بطبيعتها غير الإنسانية غير قادرة على الامتثال لهذه المبادئ الأساسية، خاصة التناسب والاحتياط، إذ يتطلبان عمليات إدراكية لا يتمتع بها إلا الإنسان، وهي حتى الآن غير قابلة للنقل إلى الآلات.

في ضوء هذا الانقسام، تتناول هذه الدراسة التحديات التي تطرحها أنظمة الأسلحة الذاتية في إطار القانون الدولي الإنساني، متبعةً نهجًا تكامليًا ثلاثي الأبعاد: مفاهيمي، قانوني، تقني–عملي. تدعم الدراسة أن أي تقييم قانوني دقيق لهذه الأسلحة لا بد أن يستند إلى فهم طبيعتها والتقنيات التي تتيح خاصية الاستقلال بها. وعليه، بينما يرتكز التحليل بشكل أساسي على قانونَي الأسلحة والاستهداف، تتطرق الدراسة إلى الجانب التقني لهذه الأسلحة لبيان كيف تُترجم الاستقلالية إلى خوارزميات وعمليات حسابية، وما هي أخطار ذلك من منظور القانون الدولي الإنساني.

وتُكمل الدراسة هذا التحليل النظري–التقني بعرض أمثلة لهذه الأنظمة ودعمها بدراسات حالة — خاصة أوكرانيا وغزة — من أجل تحليل كيفية استخدامها ميدانيًا وما تخلفه من آثار إنسانية.

تخلص الدراسة إلى أنه بالنظر للوضع التكنولوجي الحالي، لا يمكن تفويض قرارات استخدام القوة — خاصة القوة المميتة عندما يكون الهدف إنسانًا — للآلات من دون

تقويض الأطر القانونية القائمة وتعقيد المسألة القانونية حال الاستهداف والهجوم غير المشروع.

الكلمات المفتاحية: أنظمة الأسلحة الذاتية، الذكاء الاصطناعي، قانون الأسلحة، قانون الاستهداف، الاستقلالية في النزاعات المسلحة، التكنولوجيا والنزاعات المسلحة.

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
AMA	Anticipated Military Advantage
AP I	Additional Protocol I of 1977 to the Geneva Conventions
APS(s)	Active Protection System(s)
ATGM(s)	Anti-Tank Guided Missile(s)
ATR	Automated Target Recognition
AWS	Autonomous Weapon System(s)
BBC	British Broadcasting Corporation
CCW	Convention on Certain Conventional Weapons
CDE	Collateral Damage Estimation
CDEM(s)	Collateral Damage Estimation Methodologies
CIL	Customary International Law
CIWS	Close-In Weapon System
CNN	Cable News Network
DARPA	Defense Advanced Research Projects Agency
DL	Deep Learning
DoD	Department of Defense (United States)
e.g.	For example
GAI	General Artificial Intelligence
GGE	Group of Governmental Experts
GGE LAWS	Group of Governmental Experts on Lethal Autonomous Weapons Systems
HCPs	High Contracting Parties
HRC	Human Rights Council
HRW	Human Rights Watch
IACs	International Armed Conflicts
IAI	Israel Aerospace Industries
ICC	International Criminal Court
ICJ	International Court of Justice
ICL	International Criminal Law
ICRC	International Committee of the Red Cross
IDF	Israel Defense Forces
IHL	International Humanitarian Law

IPRAW	International Panel on the Regulation of Autonomous Weapons
IR	Infrarred
ISR	Intelligence, Surveillance and Reconnaissance
LARs	Lethal Autonomous Robots/Robotics
LAWS	Lethal Autonomous Weapon Systems
LIDAR	Light Detection and Ranging
LOAC	Law of Armed Conflict
MHC	Meaningful Human Control
ML	Machine Learning
NATO STO	North Atlantic Treaty Organization – Science and Technology Organization
NIACs	Non-International Armed Conflict
NPR	National Public Radio
OODA	Observe, Orient, Decide, Act
PIJ	Palestinian Islamic Jihad
RL	Reinforcement Learning
RPGs	Rocket-Propelled Grenades
SEAD	Suppression of Enemy Air Defenses
SIPRI	Stockholm International Peace Research Institute
UAVs	Unmanned Aerial Vehicles
UCASs	Unmanned Combat Aerial Systems
UK	United Kingdom
UN	United Nations
UNIDIR	United Nations Institute for Disarmament Research
UNODA	United Nations Office for Disarmament Affairs
UNSMIL	United Nations Support Mission in Libya
US	United States of America
USSR	Union of Soviet Socialist Republics
UV	Ultraviolet

INTRODUCTION

1. SETTING THE STAGE

> "[...] Considering:
> That the progress of civilization should have the effect of alleviating as much as possible the calamities of war; [t]hat the **only legitimate object** which States should endeavour to accomplish **during war** is to **weaken the military forces of the enemy**; [t]hat for this purpose it is sufficient to disable the greatest possible number of men; [t]hat **this object would be exceeded by the employment of arms which uselessly aggravate the sufferings of disabled men, or render their death inevitable**; [t]hat the **employment of such arms would, therefore, be contrary to the laws of humanity**; [...]"
> – Declaration of St. Petersburg, 1868.[1]

"Robots" — "War". This was my starting point for explaining the focus of this research — "Autonomous Weapon Systems" (AWS) — to non-specialists. Surprisingly, those two simple words elicited, almost invariably, the same reaction, irrespective of my interlocutor's race, gender, nationality, religion, social status, or academic background; and irrespective of their views on or engagement with ongoing armed conflicts: a momentary spark of interest followed by deepening confusion and concern.

---

[1] Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight. Saint Petersburg, 29 November/11 December 1868, accessible at : https://ihl-databases.icrc.org/en/ihl-treaties/st-petersburg-decl-1868/declaration?activeTab=; bold added.

When first confronted with the idea of AWS, like many who have not experienced war firsthand, the first instinct is to draw parallels to video games or science fiction, where such technologies are commonplace. Drawing an analogy with the known helps make sense of the unknown. In this context, the first mental image one might draw is still in the realm of fiction. There is still a cognitive distance that oversimplifies the issue: instead of human soldiers, robots will be fighting future wars.

However, it is in the moments that follow, when one realizes that, these are real-life technologies deployed in real warzones, with real consequences for real people, that the mental image gets abruptly replaced and concern and confusion take over. Instead of speculative abstraction, concrete images of destroyed cities, forced displacement of civilian populations, and an overwhelming number of civilian killings in the midst of conflict emerge.

That shift — from fictional to factual — is precisely what this research seeks to explore, through the combined use of three distinct yet complementary lenses: the conceptual, the legal, the technical-operational. Each dimension is complementary to the other: without understanding what AWS are, one cannot grasp how they are treated under international law; without understanding how they function in real-world contexts, one

cannot assess the adequacy or applicability of legal norms; and without legal clarity, their operational deployment risks exploiting normative loopholes or unfolding in a regulatory vacuum.

2. IDENTIFICATION OF THE OBJECT OF RESEARCH

AWS — also referred to as Lethal Autonomous Weapon Systems (LAWS) — do not possess a universally agreed-upon definition. In fact, despite over a decade of negotiations at the United Nations (UN), states remain deeply divided on even the foundational question of what qualifies as an "autonomous weapon."[2] This lack of consensus renders the task of their conceptualization, and by extension, their regulation highly disjointed and division-driven.

[2] See A. Guterres, *Lethal Autonomous Weapons Systems : Report of the Secretary-General*, UN Secretary-General, A/79/88, 2024, accessible at: https://docs-library.unoda.org/General_Assembly_First_Committee_-Seventy-Ninth_session_(2024)/A-79-88-LAWS.pdf, [hereinafter A. Guterres, A/79/88]; Group of Governmental Experts on Emerging Technologies in the Area of Autonomous Weapons Systems, *Non-exhaustive compilation of definitions and characterizations*, CCW/GGE.1/2023/CRP.1, 2023, accessible at: https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_CRP.1_0.pdf, [hereinafter, GGE, CCW/GGE.1/2023/CRP.1].

As this study will show in the following Chapters, the absence of consensus over a universal identification of what constitutes an AWS is not merely semantic or terminological; rather, it reflects a deeper divergence and a different understanding of the nature and characteristics of these systems, across states, institutions, and academic doctrine. A consequence of this divergent understanding is that, as a variable, it inherently affects the outcome and accuracy of any legal assessment regarding AWS.

To illustrate and to overcome the obstacle posed by the absence of a universal definition, we will provisionally rely on the first two institutional definitions given to AWS. The first, from the United States (US) Department of Defense (DoD), in its Directive 3000.09 "Autonomy in Weapon Systems" of November 2012, defines an AWS as a "weapon system that once activated, can select and engage targets without further intervention by a human operator."[3] The second, from the 2013 report of Christof Heyns, then United Nations Special Rapporteur on extrajudicial, summary or arbitrary executions, echoes this definition, defining Lethal Autonomous Robotics

[3] U.S. Department of Defense, *DoD Directive 3000.09: Autonomy in Weapon Sytems*, 2023, p. 21, accessible at: https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf,

(LARs) as weapon systems capable — once activated — of selecting and engaging targets without further human intervention.[4]

It appears from these definitions that a weapon system is considered an AWS if it is capable of selecting and engaging targets without human intervention beyond the initial launch. In other words, once the system has been activated, it is the weapon itself that chooses whom, what, and when to attack. This capacity to "sense–think–act" on lethal force potentially removes humans from the immediate decision-making loop, and risks violating international humanitarian law (IHL) and creating accountability vacuums.[5]

This challenge — the removal of human judgment in decisions over the use of force — is at the core of the AWS debate, particularly from an IHL perspective.

As emphasized in the Saint Petersburg Declaration of 1868, the primary objective of war is to "weaken the military forces of the enemy." This objective, however, is not absolute; it

[4] C. Heyns, *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions*, UN Human Rights Council, A/HRC/23/47, 2013, p. 1 and p. 7, accessible at: https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-47_en.pdf, [hereinafter C. Heyns, A/HRC/23/47].
[5] Ibid. pp. 7-8 and pp. 14-15.

remains limited by the "laws of humanity". In this sense, actions and decisions on battlefields must respect the targeting principles: distinction must be made between combatants and civilians, as well as military objectives and civilian objects, at all times.[6] Proportionality must be assessed against the concrete and direct military advantage anticipated.[7] Precautionary measures, when feasible, must be taken to avoid or minimize human suffering.[8] These rules are codified in Additional Protocol I (AP I) to the Four Geneva conventions and are widely recognized as customary international rules.

Thus, when considering AWS from an IHL perspective, a primary question arises: are these non-human entities capable of complying with these rules? Building on that question, would the use of these weapons "alleviat[e] as much as possible the calamities of war", or, on the contrary, "aggravate the sufferings" and "render [...] death inevitable"?[9]

As will be demonstrated through this analysis, there is no clear-cut *legal* answer to either of these questions. First, due to the previously mentioned lack of consensus regarding their identification, it follows that at least three definitional

[6] Articles 48 and 51(2) of Additional Protocol I of 1977.
[7] Articles 51(5)(b) and 57(2)(a)(iii) of Additional Protocol I of 1977.
[8] Articles 57 and 58 of Additional Protocol I of 1977.
[9] Saint Petersburg Declaration, op. cit.

approaches exist for AWS: a human-centric approach, a task-centric approach, and a technology-centric approach, each focusing on distinct elements in defining them. Among these approaches, there are different spectrums and degrees as to what constitutes "autonomy" in weapon systems, rendering the identification of the object of the debate a complex challenge. Perhaps, an adequate representation of this intangled web of perceptions, points of view, and opinions is Chris Jenks' statement "the international community cannot even agree about what they disagree about".[10]

Second, it is worth noting that across all three approaches, AWS — in the narrow sense — are reportedly not yet existent. The technologies that would enable a weapon system to act in complete autonomy and exercise cognitive judgment have not yet been fully developed. Therefore, any current or past intellectual engagement with fully AWS is inherently hypothetical and speculative — including this research. It is also inherently subjective to some extent because it relies on the choices states, institutions, scholars, experts, and researchers make in conceptualizing them.

[10] C. Jenks, *False Rubicons, Moral Panic, & Conceptual Cul-De-Sacs: Critiquing & Reframing the Call to Ban Lethal Autonomous Weapons*, Pepperdine Law Review, Vol. XLIV: 1, 2016, p. 13.

3. *L'ÉTAT DES LIEUX* OF THE DEBATE AND RELEVANCE OF THE RESEARCH

The topic of AWS is not new.[11] It began to gain significant attention within the international community in the early 2010s, particularly around 2012. This surge in interest was sparked by rapid development in drone technology and other unmanned systems, as well as advancements in artificial intelligence (AI), which made the prospect of fully autonomous weapons more plausible.

AWS first gained momentum in November 2012, when Human Rights Watch (HRW) and the Harvard Law School International Human Rights Clinic released a report titled "*Losing Humanity: The Case Against Killer Robots*".[12] This report argued that fully autonomous weapons could violate IHL and human rights principles, as they would lack the ability to make ethical decisions or distinguish between combatants and

[11] For a detailed timeline of the development of the debate and key milestones, see: United Nations Office of Disarmament Affairs (UNODA), *Timeline of LAWS in the CCW*, n.d., accessible at: https://disarmament.unoda.org/timeline-of-laws-in-the-ccw/; Autonomous Weapons, *Milestones in the Global Legal Framework for Autonomous Weapons*, 2025, accessible at: https://autonomousweapons.org/global-legal-framework-milestones/.

[12] Human Rights Watch and Harvard Law School's International Human Rights Clinic, *Losing Humanity The Case against Killer Robots*, 2012, accessible at: https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots [hereinafter HRW, Losing Humanity].

civilians. It warned that weapons able to select and engage targets without human intervention would pose grave ethical and legal risks and lack of accountability for unlawful harm. The report therefore called for a preemptive ban on such weapons.[13]

The previously mentioned report of the UN Special Rapporteur on extrajudicial, summary or arbitrary executions in 2013, represents the first time AWS were formally introduced within the framework of the UN. The report argued that the chaotic nature of armed conflict, especially in urban settings or asymmetrical conflicts, makes reliable target discrimination challenging for machines.[14] Furthermore, automated systems may struggle with context-dependent factors or with dynamic adjustments on the battlefield, as they lack the capacity to exercise human judgement to assess civilian harm in relation to anticipated military advantage.[15] Additionally, if a LAR commits an unlawful killing, it remains unclear who bears responsibility — software engineers, manufacturers, operators, or commanders. The report thus warns of a potential accountability vacuum, where no individual or entity can be straightforwardly held criminally liable.[16]

[13] Ibid. p. 46.
[14] C. Heyns, A/HRC/23/47, op. cit., p. 13.
[15] Ibid. pp. 13-14.
[16] Ibid. pp. 14-15.

The call for a preemptive ban has been increasing since then. In 2015, the AI and scientific community issued a high-profile open letter warning of the imminent reality of autonomous weapons. This letter was signed by thousands of researchers, AI pioneers, developers and private sector investors, and cautioned that AI-powered weapons risk becoming the third revolution in warfare — after gunpowder and nuclear arms.[17] The letter further urged the UN to outlaw offensive autonomous weapons beyond meaningful control, lest their deployment spark an arms race and global proliferation.[18] This was followed by another letter from founders of 116 AI and robotics companies, sent to the UN in 2017, urging a ban on autonomous weapons and warning that LAWS could be "weapons of terror," and that opening this "Pandora's box" risked precipitating a dangerous arms race.[19]

[17] Future of Life Institute, *Autonomous Weapons Open Letter: AI & Robotics Researchers*, announced at the IJCAI 2015 conference, accessible at: https://futureoflife.org/open-letter/open-letter-autonomous-weapons-ai-robotics/#:~:text=Autonomous%20weapons%20select%20and%20engage,after%20gunpowder%20and%20nuclear%20arms.

[18] Ibidem.

[19] Future of Life Institute, *An Open Letter to the United Nations Convention on Certain Conventional Weapons*, released during the International Joint Conference on Artificial Intelligence (IJCAI), 2017, accessible at: https://futureoflife.org/open-letter/autonomous-weapons-open-letter-2017/.

In an important turning point, a UN Panel of Experts report identified the first possible autonomous attack on humans in Libya's civil war in March 2020.[20] The report stated that retreated fighters were attacked by autonomous armed drone systems — reportedly attacking without needing any further human instruction or connectivity — marking the likely first case of AWS targeting people in combat.[21] The 'potential possibility' thus transformed into a concrete reality, and the urgent need to address AWS became undeniable.

Indeed, from 2021 onward, the issue of AWS has risen in prominence within UN debates. Secretary-General António Guterres has repeatedly called for a ban on fully AWS, describing them as "morally repugnant", "politically unacceptable" and concluding that they "should be prohibited by international law."[22] If the Secretary-General's position is unambiguous, the same cannot be said about states. The uncertainty shadowing AWS is reflected in the division of the

[20] UN Security Council, *Final report of the Panel of Experts on Libya established pursuant to Security Council resolution 1973*, S/2021/229.
[21] Ibid. p. 17 §63; see Chapter 3, Section 2: Autonomous Weapon Systems in recent armed conflicts.
[22] UN Press Release, *Lethal Autonomous Weapon System 'Politically Unacceptable, Morally Repugnant and Should be Banned*', Secretary-General Says during Informal Consultations on Issue, SG/SM/22643, 12 May 2025, accessible at: https://press.un.org/en/2025/sgsm22643.doc.htm.

international community over their development, and, over the normative framework to adopt for regulating them.

In this regard, three positions exist. A growing number of states — including Egypt, Austria, Pakistan, Mexico, the State of Palestine, many of the states of the Global South and some Latin American States — are calling for a ban on fully AWS and advocating the adoption of a legally binding international treaty to impose this ban. In contrast, a second position is taken by major military powers — especially, the United States, Russia and Israel — which oppose an outright ban, favor continued research and deliberation over any prohibition, and argue that the existing legal frameworks (IHL and the Convention on Certain Conventional Weapons (CCW)) are sufficient to regulate AWS. Between these two positions, a nuanced position exists, primarily assumed by China, which welcomes the discussions about a normative framework to regulate AWS and calls for a ban on the use of fully AWS, but not on their development.[23]

Despite this division, discussions are still ongoing between states within the scope of the UN (primarily through the CCW and, more recently, the General Assembly), and a prospective

[23] See Chapter 2, Section 2: The Legal Framework(s) Governing Autonomous Weapon Systems.

treaty is expected to be proposed by 2026, marking a potential milestone in the regulation of AWS,[24] and rendering this topic of urgent and time relevance.

4. ADOPTED ANALYTICAL APPROACH

For states to agree on an outright ban on AWS, there needs to be a legitimate reason for the prohibition. In this area, as will be demonstrated in this study, arguments are not lacking. Several reasons related to the dehumanization of warfare, AWS's inability to comply with IHL targeting principles, and the responsibility gap that could potentially rise from their malfunction, their misuse, or the possibility of AWS being hacked in cyberwarfare, are advanced as legitimate grounds for prohibition.

While fully acknowledging these arguments, it can be counter-argued — from a *theoretical* standpoint — that these grounds for ban are *situational* or *contextual*. In the sense that, if technology could, through its constant advancement, find solutions to overcome identified legal challenges, this situation will render obsolete the legal reasons for prohibition. In such a

[24] UNODA, *What is the position of the United Nations on LAWS?* in Lethal Autonomous Weapon Systems (LAWS), n.d., accessible at: https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/.

scenario, the assessment of AWS's compliance with IHL shall be made on a case-by-case basis, depending on the context and the effect of their use.

Further endorsing this line of thinking: if it were technologically and scientifically feasible to design and develop AWS that would not only comply, but better comply, with the law of war than humans — e.g., through precise targeting sparing civilian lives and civilian objects, reduced inhumane behavior during conflict such as rape or vengeance — would this not, conversely, mean that the use of AWS, could in the future, transform into a legal obligation?

Differently framed: if states are under the obligation to comply with the core principles of IHL — distinction, proportionality, and precaution — which require the ability to distinguish between combatants and civilians, as well as the ability to make the necessary judgements in order to minimize the effects of hostilities on civilians and civilian objects, and to continuously assess the incidental damage to civilians and civilian objects against the anticipated military advantage to determine the lawfulness of the attack — is it not possible to assume that the use of AWS can potentially transform into a legal obligation to be fulfilled as part of the obligation to take all feasible precautions to avoid and to minimize, incidental loss

of civilian life, injury to civilians, and damage to civilian objects, if they were proven to be more capable than human soldiers in achieving this aim?

These two hypothetical questions are nothing short of examples highlighting the complexity of categorically assessing AWS's compliance with IHL without accounting for contextual variables. They also suggest that the accuracy of such an assessment depends largely on technical feasibility, technological advancements, and performance assessments of specific systems in carrying out determined tasks in comparison to humans.

Thus, while the legal framework of IHL forms the normative backbone of this study, the analysis necessarily draws on interdisciplinary insights to assess how law applies to — and is challenged by — the specific nature of autonomy in weapon systems. The aim is to enrich the legal perspective with grounded technical understanding of the very systems it seeks to regulate. For this reason, a triple-lens approach is adopted, enabling a three-dimensional examination of AWS — conceptually, legally, and technically.

5. RESEARCH PROBLEM STATEMENT AND RESEARCH QUESTIONS

The emergence of AWS has triggered profound debates across legal, ethical, military, and technological spheres. Despite increasing international attention, there remains no universally accepted definition of AWS, and conceptualizations vary significantly across sources. At the technical-operational level, deployments of AI-enabled targeting and weapon systems have further highlighted the urgent need to clarify the legal implications of these systems. These deployments reveal concrete challenges in ensuring compliance with core IHL principles such as distinction, proportionality, and precaution. Furthermore, the actual capabilities and limitations of AWS vary widely across systems and across deployment contexts, complicating attempts to draw generalized legal conclusions.

Their potential to operate without human control raises questions regarding their qualification under IHL — whether they are to be treated as weapons, combatants, or as entities requiring a *sui generis* category. This, in turn, complicates the identification of applicable legal regimes and the attribution of responsibility in the event of unlawful harm. While some states argue that existing IHL frameworks are sufficient, others

contend that AWS create normative gaps that require new legal instruments, possibly in the form of a dedicated treaty.

Against this background, this research seeks to analyze AWS through three interrelated lenses, by addressing the following questions:

1. How are AWS defined across institutional and state sources, and what are the main approaches to conceptualizing them?
2. What is the legal qualification of AWS under international humanitarian law? Are they weapons, combatants, or systems requiring a *sui generis* classification?
3. What bodies of law govern AWS, and to what extent do IHL principles of distinction, proportionality, and precaution apply?
4. How have AI-enabled weapon systems been deployed in real-world conflicts, and what legal challenges have emerged from their operational use?
5. Are existing IHL rules sufficient to regulate AWS, or is there a normative gap that demands a new legal instrument?

The answer to the final question is left for the appreciation of the reader.

6. METHODOLOGY

This study adopts a doctrinal methodology combined with a structured interdisciplinary approach, both descriptive and

analytical in nature. The descriptive dimension of the methodology presents the contours and parameters of the legal and conceptual debates. The analytical dimension, however, goes further: it questions the assumptions behind existing definitions, examines the consistency of state and institutional positions, and evaluates the adequacy of current legal frameworks in light of technical developments. In this way, the study seeks to provide a deeper understanding of how law interacts with emerging technologies.

To support this analysis, the research draws on a broad set of sources, including:

- International treaties, such as the Geneva Conventions, the Additional Protocols, the CCW and its protocols;
- Customary international humanitarian law;
- The 2024 UN Secretary-General's Report on LAWS;
- United Nations documents, in particular, the reports and records of the CCW Group of Governmental Experts (GGE);
- State submissions to the CCW GGE;
- ICRC commentaries, studies, and position papers;
- Case law of the International Court of Justice where relevant;
- Institutional reports, in particular those of SIPRI and UNIDIR;
- Academic literature, drawing from legal and technical studies;

- Real-life conflict data involving AWS, including in Libya, Nagorno-Karabakh, Ukraine, and Gaza.

While the doctrinal and legal-theoretical frameworks provide the backbone of the analysis, this study also incorporates insights drawn from investigative journalism and conflict reporting. News articles and in-depth investigations by sources such as the BBC, CNN, Al Jazeera, The Guardian, and +972 Magazine offer valuable factual accounts and help supplement the doctrinal approach by empirical data and reporting on real-life uses of AWS.

This combined approach — doctrinal, interdisciplinary, and empirically informed — allows a layered and cumulative analysis, starting from foundational legal concepts and moving toward their application in complex real-world scenarios. It also reflects the nature of the object of the study itself: one that lies at the intersection of law, technology, and evolving patterns of warfare.

7. OBJECTIVE AND STRUCTURE OF THE RESEARCH

This study does not aim at speculating on whether AWS should be developed or banned in moral terms. Rather, it seeks to clarify what they are, how they function, what rules apply to

them, and whether those rules are adequate. In other words, the central objective of this research is to study AWS under IHL by applying a triple lens approach: conceptual, legal, and technical-operational. This structure is not merely thematic – it is methodological. By understanding what AWS are (conceptual lens), what they are legally considered to be (legal lens), and how they are built, deployed and function in armed conflicts (technical-operational lens), the study aims to provide a holistic analysis of AWS within the framework of IHL.

Accordingly, it is structured as follows:

Chapter 1: Autonomous Weapon Systems from a Conceptual Lens.

Chapter 2: Autonomous Weapon Systems from a Legal Lens.

Chapter 3 Autonomous Weapon Systems from a Technical-Operational Lens

CHAPTER 1– AUTONOMOUS WEAPON SYSTEMS FROM A CONCEPTUAL LENS

> "Definitions matter, though. Some envision autonomous weapons as simple robotic systems that could search over a wide area and attack targets on their own. […] Others hear the term "autonomous weapons" and envision machines with human-level intelligence […]. *Without a common lexicon, countries can have heated disagreements talking about completely different things"*.[25] — Paul Scharre, 2018.

As Paul Scharre[26] notes much of the confusion surrounding AWS stems from the absence of a common definitional ground. This observation holds particularly true in discussions about establishing a normative framework to govern their development and use. As such, conceptualizing AWS is not a merely semantic exercise, it is a foundational step toward their regulation. Specifically, the definitional ambiguity surrounding them complicates any inquiry into their compatibility with IHL,

[25] P. Scharre, *Army of None : Autonomous Weapons and The Future of War*, W.W. Norton & Company, New York | London, 2018, p. 345 ; *Italic* added.
[26] Paul Scharre is a prominent expert in autonomous systems. A former military officer, he currently serves as a Senior Fellow and Director of the Technology and National Security Program at the Center for a New American Security. He led the United States Department of Defense working group that drafted DoD Directive 3000.09 : https://www.cnas.org/people/paul-scharre.

as the assessment hinges on a prior understanding of what AWS are — and what they are not.

Therefore, this Chapter undertakes the task of exploring the definitional challenges surrounding AWS. It begins by providing an analytical overview of states and institutional definitions of AWS (Section 1), before turning to the definitional approaches that have emerged in legal scholarship (Section 2). By clarifying these definitional foundations, the Chapter aims to establish the conceptual framework necessary for the subsequent legal and technical analyses.

SECTION 1– DEFINITIONAL ATTEMPTS

The first step in properly identifying any 'thing' or 'object' is being able to associate its name with a description of its nature, utility, and most prominent features or characteristics. Take, for example, the term *weapon*. A weapon is any means or instrument designed or used to kill, injure, destroy, or incapacitate persons or objects.[27] It can be handheld (firearms), projectile (artillery shells), explosive (grenades or landmines), or unconventional (nuclear, biological or chemical). It can be

[27] The ICRC defines a weapon as "*any item of equipement supplied by States or armed groups to their armed forces or members so that in an armed conflict they can take violent action against the enemy* [...]", see ICRC, glossary, "*Weapons"*, ICRC Casebook, n.d., accessible at : https://casebook.icrc.org/a_to_z/glossary/weapons.

physical (a firearm or a missile), chemical (a toxic agent), biological (a virus), or even conceptual (cyber capabilities if they cause physical damage).[28]

The definition shifts when the word *system* is added. In a general sense, a system is "a combination of things or parts forming a complex or unitary whole".[29] From a technical standpoint, the International Council on Systems Engineering defines a system as "a collection of different elements that together produce results not obtainable by the elements alone".[30]

In this sense, a weapon system refers to a weapon combined with the integrated components necessary for its effective use. These components typically include delivery platforms (e.g., drone, aircraft, tank, or naval ship), sensors and other targeting technologies (e.g., radar, infrared, LIDAR), the weapon itself (e.g., a missile or a bomb), and the supporting command, control units, software, and algorithms. To illustrate : a guided missile

[28] See M. Gillis, *Disarmament A Basic Guide*, 4th ed., United Nations Office of Disarmament Affairs, New York, 2017; Médecins Sans Frontières, *The Practical Guide to Humanitarian Law*, "Weapons, Categories of Weapons", accessible at : https://guide-humanitarian-law.org/content/article/3/weapons/.

[29] A. Williams, '*Defining Autonomy in Systems : Challenges and Solutions'*, in Andrew P. Williams and Paul D. Scharre (eds), *Autonomous Systems Issues for Defence Policymakers*, NATO Communications and Information Agency, The Netherlands, 2015, p. 34.

[30] Ibid., p.35.

is a weapon, but a drone equipped with a targeting system that launches that missile is a weapon system.

The complexity intensifies when the adjective *autonomous* is added. Autonomy, in a general sense, can be defined as "having the quality of being self-governing […]; possessing a large degree of self-government."[31] From a moral-philosophical perspective, it refers to "acting, or [being] able to act, in accordance with rules and principles of one's own choosing."[32] Yet, when used in the context of AWS the term autonomy acquires different meanings that vary across disciplines (engineering, robotics, computer science, law and ethics), as "experts can have a different understanding of when a system or a system's function may or may not be deemed autonomous."[33]

In order to fully understand what is meant by autonomy in the context of AWS, it is first important to examine how different international actors — particularly states — *perceive* and *understand* them. This section focuses on definitions proposed in the framework of the United Nations discussions on AWS — namely, definitions included in states' submissions and

[31] Ibid., p. 33.
[32] Ibidem.
[33] V. Boulanin and M. Verbruggen, *Mapping the Development of Autonomy in Weapon Systems,* Stockholm International Peace Reaserch Institute (SIPRI), Sweden, 2017, p. 5

statements to the Group of Governmental Experts (GGE) of the CCW. It also occasionally refers to the 2013 report of former UN Special Rapporteur on extrajudicial, summary or arbitrary executions (A/HRC/23/47), and the 2024 report of the UN Secretary General's Report on Lethal Autonomous Weapon Systems (A/79/88). In addition, it refers to various documents of the International Committee of the Red Cross (ICRC). Although not a UN body or a state, the ICRC was one of the first institutional voices to draw attention to AWS and has significantly influenced the legal and diplomatic discourse.

A. INSTITUTIONAL DEFINITIONS

One of the most widely cited definitions of AWS is that of the ICRC, which describes an AWS as :

> Any weapon system with autonomy in its critical functions. That is, a weapon system that can select (i.e., search for or detect, identify, track, select) and attack (i.e., use force against, neutralize, damage or destroy) targets without human intervention.[34]

In other words, the ICRC understands AWS as

> Weapon systems that select and apply force to targets without human intervention. After initial activation or

[34] ICRC, *Views of the ICRC on autonomous weapon systems*, paper submitted to the Convention on Certain Conventional Weapons Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), Geneva 2016, p. 1, Accessible at : https://www.icrc.org/sites/default/files/document/file_list/ccw-autonomous-weapons-icrc-april-2016.pdf.

> launch by a person, an autonomous weapon system self-initiates or triggers a strike in response to information from the environment received through sensors and on the basis of a generalized 'target profile.'[35]

This means that once an operator activates the system, the AWS *itself* decides *when*, *where*, and *against what* to use force, based on pre-programmed target criteria. In that sense, the user does not choose, or even know, the specific target(s) and the precise timing and location of the resulting attack.[36] This loss of direct human choice over individual targets is the cornerstone of autonomy in the ICRC's definition. It highlights that such autonomy in the critical functions of selecting and engaging targets is what differentiates AWS from other weapons.

The former UN Special Rapporteur Christof Heyns defines AWS in almost identical terms — but under a different denomination *Lethal Autonomous Robotics* (LARs) — as "weapon systems that, once activated, select and engage targets without further human intervention."[37] The Special Rapporteur emphasized that the important element is that "the robot has an

[35] ICRC, *ICRC Position on Autonomous Weapon Systems, Background Paper*, Geneva, 2021, p. 2. Accessible at : https://www.icrc.org/sites/default/files/document_new/file_list/icrc_position_on_aws_and_background_paper.pdf.
[36] Ibidem.
[37] C. Heyns, A/HRC/23/47, op.cit., p. 7.

autonomous "choice" regarding selection of a target and the use of lethal force."[38] He also cautioned that the terms "autonomy" or "autonomous," when used in the context of robots, can be misleading. That is because they "do not mean anything akin to "free will" or "moral agency" as used to describe human decision-making."[39]

The two previous definitions focus essentially on the tasks or the functions that are rendered autonomous (selecting and engaging targets); they additionally specify that these functions need to be performed without any human intervention beyond launching or activation, for a weapon to be considered autonomous. Yet, they do not mention any technological features or capabilities enabling this autonomy nor provide clarifications on how it can be created in a weapon system.

Conversely, the UN Secretary-General's report on AWS of 2024 does not provide a formal definition. Nevertheless, it highlights the urgent need for states to reach an agreement on a definition or general characterization to be used for future work.[40]

Similarly, The GGE has not reached a consensus on a single formal definition. However, it listed a range of features

[38] Ibid., p. 8.
[39] Ibidem.
[40] A. Guterres, A/79/88, op. cit., pp. 5-6.

or attributes that might characterize AWS. In its 2018 report (GGE.1/2018/3), the following characterizations for AWS were enumerated:

- A system operating with neither human control after activation nor subordination to the chain of command ;
- A system capable of understanding higher-level intent and direction with the ability to take appropriate action by choosing its course of action without depending on human oversight and control, although these may still be present;
- A system capable of carrying out tasks governed by IHL in partial or full replacement of a human in the use of force, notably in the targeting cycle ;
- A system that once launched or deployed assumes a complex adaptive self-learning mode ;
- An adaptive system capable of navigating through complex environment by redefining scenarios and approaches ;
- A rules-based system able to switch to autonomous mode. A system that can select and attack targets without human intervention, in other words a system that self-initiates an attack ;
- Fully-autonomous systems, that is, unmanned technical means, other than ammunition, that are designed to carry out combat and support tasks without any participation of an operator ;
- A weapon system which can act autonomously in delivering (lethal) effects to a target and may also act autonomously in detection and target selection prior to engagement of the target. The level of autonomy can vary from basic levels of automation through a spectrum of an increasing number of autonomous functions and decreasing human control up to and including fully autonomous systems which operate

> across a range of functions without direct human control.[41]

The variety of attributes and features listed in the GGE's report is a reflection of the persistent lack of consensus among states on what constitutions an AWS. Some of these attributes focus on human involvement, distinguishing systems based on whether a human remains in the decision-making loop. Others highlight the system's adaptive capabilities (directly pointing at self-learning abilities, or even the capacity to interpret higher level intent). Importantly, these attributes are not arbitrary; they are directly drawn from states' discussions, national statements, and formal submissions made during the GGE meetings.

B. STATES DEFINITIONS

The UN Secretary-General's report stresses the need for states to reach a common understanding or general characterization of AWS to advance regulatory discussions. However, this agreement appears elusive — especially when examining the divergent national submissions to the GGE.[42] A

[41] Group of Governmental Experts on Emerging Technologies in the Area of Autonomous Weapons Systems, *Report of the 2018 session*, CCW/GGE.1/2018/3, 2018, pp. 11-12, accessible at: https://documents.un.org/doc/undoc/gen/g18/323/29/pdf/g1832329.pdf. [hereinafter, GGE, CCW/GGE.1/2018/3].

[42] CCW/GGE.1/2023/CRP.1, op. cit., accessible at: https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-

closer look at these submissions reveals three principal axes along which states definitions tend to diverge: (1) the human involvement spectrum (autonomy v. human control), (2) the significance of lethality as a defining characteristic, and (3) the technological features integrated into these systems such as self-learning, environment adaptability, or evolution.

First, regarding the human involvement spectrum, there is a disagreement on the degree of human control that distinguishes AWS from automated systems. While definitions such as those by France, Germany and China highlight the "total absence of human supervision"[43]; "absence of human

Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_CRP.1_0.pdf.

[43] République Française, *Non Paper Characterization of a LAWS*, Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), Convention on Certain Conventional Weapons (CCW), 11–15 April 2016, pp. 1-2 : "Lethal autonomous weapons systems are fully autonomous systems. LAWS are future systems: they do not currently exist. Remotely operated weapons systems and supervised weapons systems should not be regarded as LAWS since a human operator remains involved, in particular during the targeting and firing phases. Existing automatic systems are not LAWS either. LAWS should be understood as implying a total absence of human supervision, meaning there is absolutely no link (communication or control) with the military chain of command. Given the complexity and diversity of environments (particularly in urban areas) and the difficulty of building value-laden algorithms capable of complying with the principles of international humanitarian law (IHL), a LAWS would most likely possess self-learning capabilities, since it seems unrealistic to pre-program all the scenarios of a military operation. This means, for instance, that the delivery system would be capable of selecting a target independently from the criteria that have been predefined during the programming phase, in

intervention and control during the entire process of executing a task"[44]; and "comple[te] exclusion of the human factor from the decisions about their employment,"[45] as a primary characteristic for identifying AWS, others, in contrast, such as the United States and the Switzerland emphasize that human involvement does not *per se* negate autonomy : "[t]his includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the

full compliance with IHL requirements. With our current understanding of future technological capacities, a LAWS would therefore be unpredictable".

[44] Group of Governmental Experts on Emerging Technologies in the Area of Autonomous Weapons Systems, *Chairperson's Summary*, CCW/GGE.1/2020/WP.7, 2021, p. 46 "LAWS [are] weapons systems that completely exclude the human factor from decisions about their employment. Emerging technologies in the area of LAWS need to be conceptually distinguished from LAWS. Whereas emerging technologies such as digitalization, artificial intelligence and autonomy are integral elements of LAWS, they can be employed in full compliance with international law", [hereinafter GGE, CCW/GGE.1/2020/WP.7].

[45] China, *Position Paper Submitted by China*, CCW/GGE.1/2018/WP.7, 2018, p. 1 "LAWS should include but not be limited to the following 5 basic characteristics. The first is lethality, which means sufficient pay load (charge) and for means to be lethal. The second is autonomy, which means absence of human intervention and control during the entire process of executing a task. Thirdly, impossibility for termination, meaning that once started there is no way to terminate the device. Fourthly, indiscriminate effect, meaning that the device will execute the task of killing and maiming regardless of conditions, scenarios and targets. Fifthly evolution, meaning that through interaction with the environment the device can learn autonomously, expand its functions and capabilities in a way exceeding human expectations", [hereinafter GGE, CCW/GGE.1/2018/WP.7].

weapons system"[46]; "weapon systems that are capable of carrying out tasks governed by IHL in partial or full replacement of a human in the use of force."[47]

The lack of consensus over whether an AWS that functions entirely autonomously in the selection and engagement of targets, yet maintains human supervision by allowing the operator to intervene *if* needed to disrupt, abort or terminate the mission, may be considered as an AWS in the strict sense, remains highly controversial among states. As a result, the same weapon can be regarded as automated by some, while being considered autonomous by others.

Second, states differ on the relevance of lethality as a defining characteristic of AWS. Countries such as China,[48]

---

[46] U.S. Department of Defense, *DoD Directive 3000.09*, op. cit., p. 21, "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".

[47] Switzerland, *A "Compliance-Based" Approach to Autonomous Weapon Systems*, Working Paper submitted to the GGE, CCW/GGE.1/2017/WP.9, 2017, p. 6, accessible at: https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-_Group_of_Governmental_Experts_(2017)/2017_GGEonLAWS_WP9_Switzerland.pdf, [hereinafter GGE, CCW/GGE.1/2017/WP.9].

[48] GGE, CCW/GGE.1/2018/WP.7, op. cit., p. 1. In its 2018 Position Paper, China specified that AWS should include but not be limited to five basic characteristics. "*The first is lethality, which means sufficent pay load and means to be lethal*. [...]".

Pakistan,[49] and Norway[50] define AWS by their capacity to inflict lethal harm. Others, like Switzerland and the United States, align with the ICRC's definition, advocating for a broader approach focused on autonomy in critical functions, regardless of lethal outcomes.

In the same vein, the UN Secretary-General's report on AWS notes that while some states preferred the use of the term autonomous weapon systems, others insisted on lethal autonomous weapon systems, arguing that lethality is essential to reflect the system's potential for lethal force. Proponents of the former view argued that lethality results from usage rather than design, and therefore the term "lethal" lacks grounding in IHL.[51]

---

[49] Pakistan, *Elements of an International Legal Instrument on Lethal Autonomous Weapons Systems (LAWS)*, Working Paper submitted to the GGE, CCW/GGE.1/2024/WP 7, 2024, p. 2, Pakistan identified LAWS as "weapons systems which are designed to select and apply force to target(s) without human intervention after activation". It argued that the use of the word lethal means "that an autonomous weapon system which, by its design, has the capability to apply lethal force is included in the category of LAWS", regardless of the actual consequences of its use and whether the applied force results in lethal effects or not.

[50] Norway, *General Statement by Norway at the CCW*, Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), 13-17 November 2017, p. 1 "[W]eapons that would search for, identify and attack targets, including human beings, using lethal force without any human operator intervening".

[51] A. Guterres, A/79/88, op. cit., pp. 5-6.

The relevance of lethality as a defining characteristic for AWS is not purely semantic; it raises important questions about the nature and sensitivity of the task entrusted to the system. In fact, not all autonomous functions carry the same normative weight.[52] For example, autonomy may be used in navigation, surveillance, or logistics — while technically sophisticated — these uses do not raise the same ethical and legal concerns as would autonomy in target selection and engagement.[53] The disagreement is therefore not simply about what the system can do, but about what it is allowed to do without human intervention. This distinction is particularly relevant in assessing compliance with IHL. Focusing exclusively on lethality risks overlooking systems that, while not lethal in design, may enable or facilitate lethal effects. Moreover, it shifts attention away from how decision-making is exercised toward its outcomes, potentially creating blind spots in legal reviews. In other words, the focus is misplaced on whether the system

[52] See among others, P. Scharre, *Army of None*, op. cit., p. 35; N. Hayir, *Defining Weapon Systems with Autonomy: The Critical Functions in Theory and Practice*, Groningen Journal of International Law, vol. 9 (2): Open Issue, 2022 pp. 258-260, accessible at: https://ugp.rug.nl/GROJIL/article/view/38688/36250; S. Hua, *Machine Learning Weapons and International Humanitarian Law: Rethinking Meaningful Human Control*, Georgetown Journal of International Law, [vol. 51], 2019, pp. 122-123.

[53] V. Boulanin and M. Verbruggen, op. cit., p. 20.

kills, instead of whether it exercises autonomous judgment in performing functions that lead to the use of force.

Third, some states incorporate technological characteristics or cognitive capabilities into their definitions, thereby setting a high threshold for what qualifies as a truly autonomous weapon system. China's five-part criteria introduce elements such as *evolution* and *non-terminability*[54], highlighting the unpredictability and complexity of future AWS. France adopts a similar futuristic approach, stating that "LAWS are future systems : they do not currently exist"[55]. According to the French definition, AWS are described as

> [D]elivery platforms capable of moving through and *adapting to complex environments* (land, marine or aerial), and most crucially, of selecting and engaging targets entirely without human validation or communication with the military chain of command.[56]

[54] GGE, CCW/GGE.1/2018/WP.7, op. cit., p.1 " [...] Thirdly, impossibility of termination, meaning that once started there is no way to terminate the device. Fourthly, indiscriminate effect, meaning that the device will execute the task of killing and maiming regarless of conditions, scenarios and targets. Finally, evolution, meaning that through interaction with the environment the device can learn autonomously, expand its functions and capabilities in a way exceeding human expectations".

[55] République Française, Non-Paper: Characterization of a LAWS, op. cit., pp. 1-2.

[56] Ibidem.

The definition emphasizes that they would "likely need to possess self-learning capabilities to respond to unpredictable scenarios — particularly in urban environments — where pre-programmed parameters would be insufficient."[57] In that sense, for France, autonomy bypasses automation or rule-following, and entails a form of cognitive adaptability allowing the weapon to "select a target independently from the criteria that have been predefined during the programming phase."[58]

Similarly, the United Kingdom focuses its definition of autonomy on a system's capacity for "understanding higher level intent and direction."[59] In both its contributions to the GGE and national policy documents, the UK maintains this high threshold of autonomy. It perceives an AWS as one that is capable of understanding, interpreting and applying higher-level intent and direction, and from that understanding, "can decide on a course of action, from a number of alternatives, without human oversight and control, even though human presence may still exist."[60] The UK notes that such a system — currently not

[57] Ibidem.
[58] Ibidem.
[59] Ministry of Defence, *Joint Concept Note 1/18 : Human-Machine Teaming, Development, Concepts and Doctrine Centre*, United Kingdom, 2018, p. 60, accessible at: https://assets.publishing.service.gov.uk/media/5b02f398e5274a0d7fa9a7c0/20180517-concepts_uk_human_machine_teaming_jcn_1_18.pdf.
[60] Ibidem.

yet existent — would exhibit a sophisticated perception of its environment, and its output might be unpredictable.[61] Such definitions imply that AWS would be sophistically designed as to perform tasks that are traditionally entrusted to human *combatants*. This understanding of AWS, as will be demonstrated in the next Chapter, blurs the line between two distinct IHL categories, subject to two different legal regimes: weapons and combatants.

Importantly, the significance of these definitions lies not only in how they describe AWS, but in what they exclude. France, China, and the United Kingdom each articulate a futuristic definition of AWS, emphasizing that true autonomy will only arise when systems are capable of navigating complex environments, adapting missions, and interpreting objectives at a high cognitive level — capacities that remain beyond the reach of today's AI and robotics. This threshold renders most existing systems outside the scope of AWS as understood by these states.

Conversely, under the broader approach adopted by the United States, Switzerland, Egypt, and other states aligning with the ICRC's definition, it is sufficient for a weapon system to be capable of selecting and engaging targets, without human

[61] Ibidem.

intervention beyond activation, for it to qualify as an AWS. The threshold set by this approach is relatively low, it does not require the complete exclusion of human involvement, nor does not explicitly demand cognitive capacities or the integration of sophisticated AI or software for a system to be considered as autonomous. Under this broader framing, AWS encompass both systems that function entirely without human intervention, and those that function autonomously while still allowing for human oversight — such as the ability to abort, override or terminate the mission. This understanding makes AWS not a hypothetical future concern, but a present-day reality.[62]

The divergences observed across institutional and state definitions reveal more than terminology differences — they reflect fundamentally distinct ways of conceptualizing autonomy in weapon systems.

SECTION 2– DEFINITIONAL APPROACHES

Given the diversity of definitions examined, it becomes clear that the real point of contention lies less in the wording

[62] P. Scharre, Army of None, *op. cit.*, p. 101, citing Former Deputy Secretary of Defense Bob Work : "*We, the United States, have had a lethal autonomous weapon [...] since 1945: the Bat [radar-guided anti-ship bomb].*"; see Chapter 3–Secion 2 of this study.

itself and more in the underlying assumptions about what matters most when defining autonomy in weapons systems.

The United Nations Institute for Disarmament Research (UNIDIR) identifies three competing definitional approaches for AWS which are "complementary if sequenced correctly."[63] First, there is the human-centric approach, which describes AWS in relation to a human user. Second, there is the functional (task-centric) approach, which focuses on identifying the tasks or functions performed autonomously by the weapon. Third, there is the technology-centric approach which covers technical definitions in which the weapon itself is technologically described.[64]

A. THE HUMAN-CENTRIC APPROACH

In the 2024 Compilation of replies to the Chair of the CCW GGE, the term "human" appeared 197 times. More specifically, "human control" was mentioned 48 times alongside with the terms "human intervention", "human involvement", "human

[63] UNIDIR, *The Weaponization of Increasingly Autonomous Technologies: Concerns, Characteristics and Definitional Approches*, UNIDIR Ressources No. 6, 2017, p. 21, accessible at: https://unidir.org/wp-content/uploads/2023/05/the-weaponization-of-increasingly-autonomous-technologies-concerns-characteristics-and-definitional-approaches-en-689.pdf.
[64] Ibid., pp. 19-22.

oversight", and "human supervision."[65] This observation highlights the centrality of the human-machine relationship in multilateral discussions about AWS. Autonomy, in this context, means delegating some level of control/decision-making to an object.[66] The human-centric approach thus relies on determining the degree of human control over a weapon regardless of the degree of automation.[67]

Thomas Christian Bächle and Jascha Bareis note that, according to this approach, weapon systems are to be called autonomous if they minimize the potential for human intervention to the point where that control is no longer required or even allowed at all.[68] In this sense, this approach reflects a relational conception of autonomy, defined by the extent to which human intervention and agency remain possible.[69]

---

[65] Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, *Compilation of Replies Received to the Chair's Guiding Questions*, CCW/GGE.1/2024/CRP.1, 2024, accessible at : https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2024)/CCW_GGE1_2024_CRP1.pdf.

[66] UNIDIR, *The Weaponization of Increasingly Autonomous Technologies: Concerns, Characteristics and Definitional Approaches,* op. cit., p. 20.

[67] T.C. Bächle and J. Bareis, op. cit., p. 4.

[68] Ibidem.

[69] Ibidem.

The UNIDIR Report *The Weaponization of Increasingly Autonomous Technologies: Concerns, Characteristics and Definitional Approaches* highlights the benefits of this approach, particularly in states level discussions, as it provides a common language for discussion that is accessible to a broad range of governments and publics regardless of their degree of technical knowledge; it focuses on the shared objective of maintaining some form of control over all weapon systems; it is consistent with IHL regulating the use of weapons in armed conflict, which implicitly entails a certain level of human judgment and explicitly assigns responsibility for decisions made; and it is a concept broad enough to integrate consideration of ethics, human-machine interaction and the 'dictates of the public conscience', which can be marginalized in approaches that narrowly consider just technology or just law.[70]

Despite its importance, the ICRC recognizes that there is no universal model for optimal human-machine interaction with autonomous systems, since the need for human control, or the level of autonomy that can be tolerated, is linked to the complexity of the environment in which the system operates and

[70] UNIDIR, *The Weaponization of Increasingly Autonomous Technologies: Concerns, Characteristics and Definitional Approaches,* op. cit., pp. 20-21.

the complexity of the task it carries out.[71] The report adds that generally, the greater the complexity the greater the need for direct human control and less the tolerance of autonomy, especially for tasks and in environments where a system failure could kill or injure people or damage property, i.e., "safety-critical" tasks.[72]

It should be noted that the ICRC, as well as the International Panel on the Regulation of Autonomous Weapons (IPRAW), distinguish two types of human control : "control by design" (i.e., in design and development) and "control in use" (i.e., in activation and operation).[73] Both types of control are equally important in the context of AWS, but each focuses on a different role for the human in a different stage of the life cycle of the weapon. In the control by design phase, focus is on the pre-deployment phase, where the role of human refers to the role of the developers, programmers, and manufacturers. In contrast, in the control in use phase, focus is shifted to the human operators and/or commanders. Their role in the deployment and actual operation of the weapon is fundamental for assessing compliance with the core principles of IHL while the weapon is

[71] ICRC, *Autonomy, artificial intelligence and robotics : Technical aspects of human control,* op. cit., p. 8.
[72] Ibidem.
[73] Ibid., pp. 7-8.

being used. The effective combination of both types of control ensures that any developed weapon, whether autonomous or not, complies with international law.

In the context of AWS, the ICRC notes that human control over robotic systems during operation can take several forms. First, there is *direct control*, which requires constant intervention by a human operator to directly or remotely control the functions of the system — systems under such control are therefore not autonomous (non-autonomous or inert systems). Second, there is *shared control*, which means that the human operator directly controls some functions, while the machine controls other functions under the supervision of the operator– these systems are often referred to as *semi-autonomous* systems. An example is armed drones, where a human operator directly (albeit remotely) controls the critical targeting functions, while the machine autonomously controls flight and navigation functions, under human supervision. Third, there is *supervisory control* — also referred to as *supervised autonomy* — where a robotic system performs tasks autonomously while the human operator supervises and can provide instructions and/or intervene and take back control, if necessary.[74] This type of control requires prior knowledge of how the system will

[74] Ibid., p. 8-9.

function in the future and how the environment may evolve, enabling the user to judge when intervention will be necessary and in what form.[75] Finally, when human control is inexistent after activation, i.e., when the system independently selects and engages targets without real-time oversight or input from a human operator — these systems are referred to as *fully autonomous* weapon systems and are the most ethically and legally problematic.

Today, the human-machine relationship is commonly framed in terms of the human's position relative to the 'loop'.[76] The term loop refers to the decision-making cycle involved in the use of force — particularly in the sequence of sensing, processing information, making a decision, and acting — often referred to in military doctrine as the OODA loop (Observe–Orient–Decide–Act).[77]

[75] Ibidem.
[76] See Human Rights Watch, *Losing Humanity*, op. cit.
[77] T. Geraghty, *John Boyd and The OODA Loop*, Psych Safety, 2024, accessible at: https://psychsafety.com/john-boyd-and-the-ooda-loop/ ; J.N. Rule, *A Symbiotic Relationship: The OODA Loop, Intuition, and Strategic Thought*, Strategy Research Project, United States Army War College, 2013, pp. 5-15, accessible at: https://apps.dtic.mil/sti/pdfs/ADA590672.pdf.

A human may be *in* the loop (exercising direct control), *on* the loop (monitoring and able to intervene), or *out* of the loop (completely removed from real-time decision-making).[78]

Similarly, for Paul Scharre, there are degrees of autonomy for any given task. A machine can perform a task in a semiautonomous, supervised autonomous, or fully autonomous manner. He distinguishes three main operational models :

> • **Semi-autonomous (human-in-the-loop) :**
> In semiautonomous systems, the machine performs a task and *then waits for the human user to take an action before continuing*. A human is "in the loop". […] In semiautonomous systems the loop is broken by a human. *The system can sense the environment and recommend a course of action but cannot carry out the action without human approval*.
> • **Supervised autonomous (human-on-the-loop) :**
> In supervised autonomous systems, the human sits "on" the loop. Once put into operation, *the machine can sense, decide, and act on its own, but a human user can observe the machine's behavior and intervene to stop it, if desired*.
> • **Fully autonomous operation (human out of the loop) :**
> Fully autonomous systems *sense, decide, and act entirely without human intervention.* Once the human activates the machine, *it conducts the task without communication back to the human user*. The human is "out of the loop".[79]

Scharre further emphasizes that a system can operate in different modes at different times, and it may become "more autonomous" by increasing its autonomy along any one of these

[78] HRW, *Losing Humanity*, op. cit., p. 2.
[79] P. Scharre, *Army of None*, op. cit., pp. 36-37; *Italic* added.

spectrums.[80] This means that depending on the nature of the task, and not the global consideration of the weapon, automation, and autonomy can be exercised in varying degrees and could co-exist in the same weapon. Based on this typology, both supervised autonomous and fully autonomous weapons meet the definition of AWS capable of operating without human intervention.

Conversely, Noel Sharkey critiques the loop-based model for not guarantying the exercise of human judgment nor clarifying the depth of involvement of the human in the control loop. He argues that the role of the human could simply be limited to programming a weapon system's mission or pressing a button to activate it, or it could mean exercising full human judgment about the legitimacy of a target before initiating an attack.[81] He notes that the terms 'autonomous' and 'semi-autonomous' weapons blur the line regarding the control issue and proposes an alternative approach to the classification of autonomy in

[80] Ibid., p. 35.

[81] N. Sharkey, *The human control of weapons: a humanitarian perspective*, in N. Bhuta, S. Beck, R. Geiss, C. Kress, H. Y. Liu (eds.), *Autonomous Weapons Systems: Law, Ethics, Policy*, Cambridge University Press, Draft version, p. 3, accessible at: https://archive.law.upenn.edu/live/files/3948-sharkey---human-control-of-weapons-pf-draftpdf; see also: State of Palestine, Submission on Autonomous Weapon Systems to the United Nations Secretary-General, 2024, pp. 1-2, accessible on: https://docs-library.unoda.org/General_Assembly_First_Committee_-Seventy-Ninth_session_%282024%29/78-241-State_of_Palestine-EN.pdf.

terms of the type and quality of human control afforded by different types of computerized weapon systems.[82] In his views, the proposed classification moves away from "technical jargon to plain language"[83] and goes as follows:

> 1. Human engages with and selects targets and initiates any attack
> 2. Program suggests alternative targets and human chooses which to attack
> 3. Program selects target and human must approve before attack
> 4. Program selects target and human has restricted time to veto
> 5. Program selects target and initiates attack without human involvement.[84]

Other classifications, models and scales can be found in the legal literature beside the ones listed above — all of them have in common that they define the term autonomy by the degree of human control over specific information and decision processes.[85]

The problem with this approach is, as Merel Ekelhof notes, that there is an ambiguity regarding human control, not just over semantics and content, but more specifically over *who*

---

[82] N. Sharkey, op. cit., p. 3.
[83] Ibid., p. 4.
[84] Ibidem.
[85] C. Alwardt and M. Krüger, *Autonomy of Weapon Systems*, Institute for Peace Research and Security Policy at the University of Hamburg (IFSH), 2016, p. 2, accessible at: https://ifsh.de/file-IFAR/pdf_english/IFAR_FFT_1_final.pdf.

should exercise control and over *what*.[86] In this regard, she notes that several suggestions have been made. Those include control over every individual attack (e.g., NGO Article 36); over the ultimate decision to use force (e.g., France); over the wider loop or the targeting cycle (e.g., Netherlands, Switzerland); over the critical functions of the weapon (ICRC); or over the weapon system (e.g., Japan, Austria).[87]

Although, the human-centric approach is the most commonly used, particularly on states level discussions, it presents certain limitations. While it may be the 'simplest' in terms of conceptualizing AWS, the presence of a human *in* or *on* the loop often places us more in the realm of human-machine interaction, particularly supervisory control.[88] This configuration, in principle, raises fewer legal and ethical challenges compared to scenarios where the human is completely removed from the loop. In the latter case, we shift to the delegation of targeting and engagement decisions — or as

[86] M. Ekelhof, op. cit., p. 133.
[87] Ibidem.
[88] I. Puscas, *Human-Machine Interfaces in Autonomous Weapon Systems considerations for Human Control*, UNIDIR, 2022, accessible at: https://unidir.org/files/2022-07/UNIDIR_Human-Machine%20Interfaces.pdf; The UNIDIR report identifies multiple modalities of human-machine interaction relevant to AWS: human-centred interaction, interaction-centred design, supervisory control, and human-AI teaming.

framed in formal discussion "life-and-death decisions"[89] — entirely to the machine. This configuration raises not only profound ethical concerns but also significant challenges under international law, particularly regarding the responsibility gaps that may arise from the use of such systems.[90]

An additional problem emerges when considering systems operated with a human "*on*" the loop. The abstract understanding of this category — which may not be technically precise — refers to a slight adaptation of 'autonomy' wherein the system completes the entire targeting and engagement cycle on its own, with the human retaining the ability to intervene to cancel, abort, or terminate the mission. While this structure formally maintains a role for human supervision, it raises a legitimate question about the "meaningfulness" of that role. Can it be assumed that 'pressing a button' to stop the operation is sufficient to assert that meaningful human control was exercised over the use of force?[91]

---

[89] See A. Guterres, A/79/88, op. cit., for example: submissions from Costa Rica (p. 39), Mexico (p.74), Human Rights Watch (p.144), Stop Killer Robots Youth Network (p.170).

[90] Ibid., for example: submissions from Austria (p. 26), Bulgaria (p. 30), Canada (p. 32).

[91] In this regard, see the Submission of The State of Palestine on AWS, op. cit., p. 1-2 "[...] the need to recognise that a "nominal human input" does not amount to an intervention for the purpose of defing what an autonomous weapons system is"; p. 2 "if a human was required to press a keyboard button after the system's activation in order for force to be

B. THE FUNCTIONAL APPROACH

The functional approach highlights that referring to autonomy as a general attribute of weapon systems is imprecise — if not meaningless — since what primarily matters is the nature of the specific tasks performed autonomously by the machine, rather than the overall level of autonomy of the system as a whole.[92]

The most widespread functional definition of AWS is the previously mentioned definition by the ICRC, which defines an autonomous weapon system as "any weapon system with autonomy in its critical functions. That is, a weapon system that can select (i.e., search for or detect, identify, track, select) and attack (i.e., use force against, neutralize, damage or destroy) targets without human intervention."[93] Similarly, the US DoD defines an AWS as "a weapon system that, once activated, can select and engage targets without further intervention by a human operator."[94]

executed, without any moral or legal consideration of the consequences, would this amount to a "human intervention" [...] In other words, would the mindless click of a keyboard button by a human after the system's activation lead the system to fall outside the AWS framework [...]?".

[92] V. Boulanin and M. Verbruggen, op. cit., pp. 6-7; *Italian* added.

[93] ICRC, *Views of the ICRC on autonomous weapon systems*, op.cit., p. 1.

[94] U.S Department of Defense, *DoD Directive 3000.09*, op. cit., p. 21.

In their statements to the GGE many states adopted the functional approach. For example, Belgium stated that the discussion should focus on systems whose critical functions are autonomous.[95] Similarly, Norway and the Netherlands define AWS as weapons that would "search for, identify and attack targets, including human beings, without any human operator intervening"[96] and as "a weapon that […] selects and engages targets."[97] Accordingly, it becomes essential to identify what is meant by a weapon system's critical functions.

The Stockholm International Peace Institute (SIPRI) identified five functions for weapons with autonomy in some of

[95] Belgium, *Intervention de la Belgique*, GGE, CCW, 2018, accessible at : https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2018/gge/statements/9April_Belgium.pdf, "Il est en effet important de mieux définir les contours de notre débat. Celui-ci doit se centrer sur les Systèmes d'armement létaux autonomes, c'est-à-dire des systèmes pour lesquels les fonctions létales critiques sont autonomes. Il est dès lors préférable d'écarter des débats les fonctions autonomes non létales".

[96] Norway, *General Statement by Norway*, op. cit., p. 1.

[97] The Netherlands, *Examination of Various Dimensions of Emerging Technologies in the Area of the Lethal Autonomous Weapons Systems*, Working Paper submitted to the GGE, CCW/GGE.1/2017/WP.2, 2017, p. 1, accessible at: https://www.reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2017/gge/documents/WP2.pdf.

their functions : (1) mobility[98] ; (2) targeting[99]; (3) intelligence[100]; (4) interoperability[101]; and (5) health management[102].[103]

For the ICRC a weapon might have autonomy in certain functions without having "system-level" autonomy, i.e.,

[98] N. Hayir, op. cit., p. 258. Based on the work of V. Boulanin and M. Verbruggen, op. cit., Hayir notes that main mobility functions include homing and follow-me functions; navigation and functions related to take off-and landing. He identifies homing as the function of following a specified target and follow me is following another system or soldier. Navigation is the function that allows the system to position itself and plan/follow a route. Take-off and landing concern particularly aircrafts' operation of leaving the ground and returning to it. He argues that despite them forming a critical part of an AWS' operation, autonomy in these functions cannot be deemed critical.

[99] Ibid., p. 259. Targeting is not a single step but a process by which weapons are applied to affect addreseeses using a variety of tactics that create effects contributing to designated goals.

[100] Ibidem., These functions can be distinguished into functions related to the system's ability to handle information (e.g. detection of explosive devices, detection of intrusion by unauthorized living beings into a predefined area, detection and location of the weapon fire in terms of direction and range, surveillance and reconnaissance missions) and functions related to the system's ability to generate data (e.g. map generation, threat assessment, and use of big data analytics to find correlations and recognize patterns.

[101] Ibid., p. 260. Interoperability functions refer to the ability of the system to operate in conjuction with other systems or humans. It can be collaborative where the systems work in coordination to achieve one common goal, or for coordination in mobility, or in surveillance and reconnaissance missions.

[102] Ibid., pp. 258-259. These functions include self-recharging/refuelling; fault detection and diagnosis and self-repair.

[103] V. Boulanin and M. Verbruggen, op. cit., p. 20.

autonomy in all other functions.[104] The question therefore become what distinguishes one function from another in terms of criticality from an IHL perspective?

In fact, as previously mentioned, some functions can be made autonomous without presenting significant ethical or legal risks (e.g., mobility and navigation), while others may be a source of greater concern (e.g., targeting).[105] In this regard, Nurbanu Hayir rightly notes that the broad categorization of the ICRC of these functions as target selection and engagement, does not correctly capture the nuances that might lead to an IHL violation. He gives the example of intelligence functions, particularly those related to provision of information, which may be critical and influence targeting. He argues that "[t]o the extent that these functions form an integral part of the interaction between the weapon system and the targets, they will be critical, and assessment must be made for each function *in casu*".[106]

In other words, intelligence functions can be deemed critical if engagement with the target depends on the information gathered by the system as they might form an

[104] ICRC, *Autonomy, artificial intelligence and robotics : Technical aspects of human control,* op. cit.*,* p. 5.
[105] V. Boulanin and M. Verbruggen, op. cit., pp. 6-7.
[106] N. Hayir, op. cit., p. 259.

integral part to the engagement process.[107] While this insight is essential and will be revisited in the operational analysis in Chapter 3,[108] the present discussion follows the prevailing consensus centered on the targeting function — in particular, the autonomous selection and engagement of targets.

Merel Ekelhof emphasizes that terms like "select" and "engage", often referred to as the "critical functions" of autonomous weapons, are not as straightforward as they may seem.[109] For instance, "select" can be used narrowly to mean target recognition (e.g., detecting a radar signature), just as much as it can refer to more complex processes of target planning and prioritization. Similarly, the meaning of "attack" (engage) is also ambitious, does it refer to a single act of force, or can it include multiple applications over time and space?[110]

---

[107] Ibid., p. 260.

[108] See Chapter 3–Section 2, providing examples from real-life armed conflicts; particularly, "the Gospel" and "Lavander", AI-empowered targeting systems used in the armed conflict in Gaza to identify and select potential Hamas targets.

[109] M. Ekelhof, *The Distributed Conduct of War: Reframing Debates on Autonomous Weapons, Human Control and Legal Compliance in Targetin*g, PhD-Thesis, Vrije Universiteit Amsterdam, 2019, p. 74-75, accessible at: https://research.vu.nl/ws/portalfiles/portal/90547665/complete%20dissertation.pdf.

[110] Ibid., p. 75.

Heather Roff builds on this ambiguity to distinguish automatic from autonomous systems based on the meaning of "select". She notes that in some cases, select may refer to scanning a given space for specific sensor inputs. However, in such instances, the system is not truly selecting a target on its own; rather, it is searching for a preselected target based on parameters defined by a human operator. In this sense, it is the human who has selected the target — either by programming the criteria or by designating a specific object or area. Consequently, a weapon operating this manner should be considered automatic, not autonomous.[111]

For her what distinguishes autonomous weapons from automatic weapon is that automatic weapons — however sophisticated they are — are incapable of learning, or of changing their goals. Conversely, "limited learning weapons"[112] are capable both of learning and changing their sub-goals while deployed. They truly select a target among a range of objects or persons.[113]

[111] H. Roff, *Distinguishing autonomous from automatic weapons*, Bulletin of the Atomic Scientists, 2016, accessible at: https://thebulletin.org/roundtable_entry/distinguishing-autonomous-from-automatic-weapons/
[112] Ibidem.
[113] Ibidem.

The functional approach is compelling in that it defines AWS through the lens of specific functions, especially those deemed critical. Yet, the operationalization of functional definitions depends on the assumptions made about the human role in the loop, as well as on how the parameters of automation are drawn and the criteria used to distinguish automated from truly autonomous weapons from a technical standpoint.

C. THE TECHNOLOGY-CENTRIC APPROACH

The technology-centric approach focuses on autonomy as a technical feature, rather than treating AWS as a distinct category of weapons. Under this approach, autonomy is understood as the actual ability of a system "to exercise control over its own behaviour (self-governance) and deal with uncertainties in its operating environment."[114]

Thomas Christian Bächle and Jascha Bareis describe this approach as a technical approach to defining autonomy, which focuses of the attribute of autonomy itself as a determining and distinguishing feature.[115] In that sense, an AWS is a system that, drawing on collected data and operating within pre-defined

[114] V. Boulanin and M. Verbruggen, op. cit., p. 6.
[115] T.C. Bächle and J. Bareis, *"Autonomous weapons" as a geopolitical signifier in national power play: analysing AI imaginaries in Chinese and US military policies*, European Journal of Futures Research, SpringerOpen, 2022, p. 3

constraints, is capable of independently selecting and engaging targets.[116] This distinguishes them from automated systems which are only "triggered" based on case-specific inputs but lack the capacity to make autonomous target decisions.[117]

It should be noted that, the technology-centric approach primarily relies on the distinction between *automatic*, *automated*, and *autonomous* systems. For example, Paul Scharre frames this approach in terms of the "sophistication of the machine's decision-making when performing a task."[118] According to him, automatic systems are simple machines that exhibit minimal, if any, decision-making capabilities. They sense their environment and respond in a direct and linear manner, rendering the connection between input and output immediate and highly predictable to the user.[119] Automated systems, by contrast, are more complex: they may process a

[116] Ibidem.; citing R. Crotoof, *The Killer Robots Are Here: Legal and Policy Implications,* Cardozo Law Review, vol. 36 (1837), 2015, pp. 1854-1862.
[117] T.C. Bächle and J. Bareis, op. cit., p. 3.
[118] P. Scharre, *Army of None*, op. cit., pp. 34-35. Scharre notes that when analyzing autonomy in weapon systems, three different dimensions should be considered independently : (1) the type of task the machine is performing; (2) the relationship of the human to the machine when performing that task; and (3) the sophistication of the machine's decision-making when performing the task. He refers to this last dimension as the "spectrum of intelligence in machines."
[119] Ibid., p. 38.

range of inputs and weigh multiple variables before executing an action. However, their internal cognitive processes remain generally traceable and comprehensible to a trained human user, at least in principle.[120] Finally, autonomous systems are those advanced enough that their internal decision-making processes are no longer easily intelligible to the human user. He emphasized that while the user understands the objective the system is supposed to fulfill, they may not fully grasp how the system will go about achieving it. The reason behind this is that these systems are goal-oriented: the human sets the goal, but the system has the discretion and flexibility to determine how to accomplish it.[121]

Similarly, Vincent Boulanin and Maaike Verburggen maintain this distinction and define an autonomous system as one — whether hardware or software — that, once activated, can perform some tasks or functions without human involvement. This is made possible through its interaction with the environment, relying on sensors and programmed responses.[122] In their view, what sets it apart from an automatic system is its capacity to compose and evaluate multiple possible

[120] Ibidem.
[121] Ibid., p. 39.
[122] V. Boulanin and M. Verbruggen, op. cit., p. 123.

actions and select among them based on its understanding of itself, the world, and the specific context in which it operates.[123]

The distinction between automatic, automated and autonomous, while conceptually useful, is in practice difficult to measure and to determine whether a system falls within one of the three categories.[124] The plain understanding of each of these categories shows that the machine responds without direct human intervention in all three cases; the difference lies in the degree and parameters of control exercised by the human over the decision-making process — if any.

Additionally, AWS cannot be considered in isolation from their operational domain, i.e., the environment in which the system is deployed. Former UN Special Rapporteur Christof Heyns distinguishes "automation" from "autonomy" based on environmental complexity. According to him, automatic

[123] Ibidem.

[124] For example the Phalanx Close-In Weapon System (CIWS) or the Iron Dome are in principle labeled automatic or automated because they automatically detect and intercept incoming missiles. However, having different levels of automation led some to argue they are autonomous in function when operating without human input. In that sense, they can behave as autonomous depending on operational settings. Similarly, when a drone is programmed to follow predefined waypoints it is considered automated, but if it is equipped with machine learning-based object recognition allowing it to adjust its flight to avoid obstacles or reclassify targets in real-time, its responses are no longer pre-coded but adaptive blurring the line between automated and autonomous.

systems, such as household appliances, operate within a structured and predictable environment. Conversely, "autonomous systems can function in an open environment, under unstructured and dynamic circumstances".[125]

The environmental complexity is particularly important when assessing AWS' compliance with IHL, because what may be problematic in a particular environment (e.g., urban or civilian populated environment) might be less so in a different environment (e.g., under the sea or in space), where risks to civilians are minimal or non-existent. The more complex the environment, the harder it becomes to reliably increase autonomous functioning without risking the violation of IHL core principles.

Furthermore, from a technical standpoint, what determines the level or the degree of autonomy of a system is primarily the sophistication of its software. Software systems — whether AI-enabled or not — could directly activate a weapon, making it autonomous.[126] These can range from basic algorithms (deterministic, rule-based, "if-then" rules) to highly

[125] C. Heyns, A/HRC/23/47, op. cit., p. 8.
[126] ICRC, *Autonomy, artificial intelligence and robotics : Technical aspects of human control*, 2019, p. 6, accessible at: https://www.icrc.org/sites/default/files/document/file_list/autonomy_artificial_intelligence_and_robotics.pdf.

complex algorithms (probabilistic, AI-enabled — particularly by "machine-learning" (ML)).[127] Although, existing weapon systems function by collecting information, processing it through software, and then acting based on what they were programmed to do. The advent of AI, particularly ML, makes these systems no longer solely relying on pre-programming; instead, they can adapt their behavior and action by themselves, "they "learn" how to do a task through training, use, and user feedback."[128]

These learning and adaptive capabilities are emphasized in both, China and France's definitions of LAWS.

> "[…Fifthly evolution, meaning that through interaction with the environment the device *can learn autonomously, expand its functions and capabilities in a way exceeding human expectations*."[129]

> "[…] The delivery platform of a LAWS would be capable of moving, adapting to its land, marine or aerial environments and targeting and firing a lethal effector (bullet, missile, bomb, etc.) without any kind of human intervention or validation. […] *LAWS would most likely possess self-learning capabilities*."[130]

---

[127] See Chapter 3 - Section 1: The internal architecture and technological foundations of autonomous weapon systems.
[128] S. Hua, op. cit., p. 118.
[129] GGE, CCW/GGE.1/2018/WP.7, op. cit., p. 1; *Italic* added.
[130] République Française, Non-Paper: Characterization of a LAWS, op. cit., p. 2; *Italic* added.

As such, autonomy should ultimately be understood as a set of features or upgrades that can be added to any weapon system. The ICRC report *Autonomy, artificial intelligence and robotics: Technical aspects of human control* underscores this point, noting that "[t]oday's remote-controlled weapons could become tomorrow's autonomous weapons with just a software upgrade".[131]

While the technology-centric approach offers an understanding of AWS through the internal architecture of a system and its operational complexity, it does not capture the implications of how such a system is used and what roles it performs in military operations. Two systems with similar technical capabilities may have radically different legal qualification depending on their function, mode of deployment, and level of human oversight.

***

Taken together, these divergent perspectives reveal that what matters is not only whether a human is 'in' or 'on' the loop, but whether their presence allows for informed and accountable decisions in the use of force. For centuries, war has been defined as a fundamentally human endeavor, with decisions over life-

[131] ICRC, *Autonomy, artificial intelligence and robotics : Technical aspects of human control*, op.cit., p. 6.

and-death made by individuals capable of moral judgment, empathy, and accountability. The introduction of AWS signals a potential shift in this paradigm: the gradual transfer of decision-making authority from humans to machine. This transition is not without consequences, it raises profound questions about whether the legal foundations of warfare, built on human judgment and responsibility, can be upheld when critical decisions are delegated to algorithms. It is therefore necessary to turn next to how AWS are examined under international law — specifically, under international humanitarian law.

CHAPTER 2– AUTONOMOUS WEAPON SYSTEMS FROM A LEGAL LENS

The *Oxford Handbook of the Use of Force in International Law* enumerated three existing approaches to peace and war, which perfectly illustrate the inherent link between humans and war.[132] The contemporary international order reflects elements from these three approaches — realist[133],

[132] M. Weller, *Introduction: International Law and the Problem of War*, in M. Weller (ed.), The Oxford Handbook of the Use of Force in International Law, Oxford University Press, 2015, pp. 4-6.

[133] Ibid., pp. 5-6. The "realist approach" considers that "human beings are inherently prone to organized violence"; they "carry the seeds of war within their genetic codes". Accordingly, "Si vis pacem para bellum" (if you want peace, prepare for war) (p.4). War can only be avoided by the threat of war. In the shadow of this approach, rules and customs of warfare developed over time. Notably, with the emergence of the concept of Just War, then by the adoption of rules governing the conduct of belligerents, and the introduction of rules on arms control as an attempt to achieve strategic stability between states and alliances. Particularly, the second half of the 20th century showed a significant extension of arms control, seeking to outlaw the possession or use of certain types of weapons and to limit the use of others and to limit the spread of nuclear weapons, while supporting the doctrine of nuclear deterrence or mutually assured destruction. Under this approach, law is perceived as a "tactical undertaking", linking the avoidance of war and the limitation of its effects to "where all involved were interested" and this outcome was in "the mutual interest of all".

managerial,[134] and idealist,[135] — each placing the human being at the center of the discourse on war and peace. Across each of these perspectives, the regulation of force, the pursuit of peace, and the legitimacy of war have remained rooted in human faculties: conscience, judgment, agency, and responsibility. Humans remained at the center of both, *jus ad bellum* (the law of use of force) and the *jus in bello* (the law of war). However, the rapid development of technologies capable of exercising autonomous functions in warfare introduces a potential rupture

[134] Ibid., p. 6. The "managerial approach" views that human beings may not necessarily be warlike by their very nature. However, it is the organization into states that "turns mankind into its own wolf". In other words, organized societies develop the technology and capacity to wage war and compete for scarce resources (mostly land, labour and strategic resources). Therefore, the drive towards war is not inherent in the human condition, but in human organization. The proponents of this approach argued that if presented with alternative means of settling disputes, humans constituting states, would not rationally choose war. This approach encouraged the creation of alternative mechanisms of resolving conflicts between states in the ultimate goal of avoiding the resort to war. Those mechanisms included International Organizations, the Permanent Court of Arbitration, the International Court of Justice, among other mechanisms.

[135] Ibidem. The "idealist" or "utopian approach" considers war as a culturally learnt behavior, by societies coming into contact with one another. This means that it can potentially be unlearnt. War would, thus, no longer be perceived as an agent of national advancement and a measure of cultural achievement, instead, it would be painted as the "ultimate cultural failure" and "simply irrational", signaling the need for a collective act of will to abolish war as an acceptable form of human interaction. The main loophole of this approach remains that the system cannot operate unless it is universally shared. So long as war remains possible to the minds of some, the others will tend to feel the need to be prepared for defense.

in this long-standing human-centric paradigm, particularly, under the *jus in bello*.

International Humanitarian Law, also known as the Law of Armed Conflict (LOAC), and previously referred to as the Law of War, is a specialized branch of international law[136] that developed over centuries — drawing on religions, moral codes, customs — and peaked with the adoption of the Four Geneva Conventions of 1949 and their Additional Protocols, particularly Protocols I and II of 1977. Its primary aim is to limit the effects of warfare by protecting persons who are not participating in hostilities and by restricting the means and methods of warfare.[137]

This means that unlike the *jus ad bellum*, IHL is not concerned with the motives or legality of waging war but seeks to humanize armed conflict and minimize non-military damages

[136] See among others: H. Atlam, *Law of International Armed Conflicts*, Dar Al-Nahda Al-Arabia, 2003 (in Arabic); H. Atlam, *Lectures in International Humanitarian law*, ICRC, Cairo, 2010 (in Arabic); C. Atlam and O. Mekki, *Guide for Judges on International Humanitarian Law: Volume II*, ICRC, Geneva, 2015 (in Arabic); S. Amer, *Introduction to the Study of the Law of Armed Conflicts*, Dar Al-Fekr Al-Arabi, Cairo, 1977 (in Arabic); M. Safi Youssef, *The Mediator in International Humanitarian Law*, Dar Al-Nahda Al-Arabia, 2024 (in Arabic); J. Pictet, *Développement et principes du droit international humanitaire*, Pedone, Paris, Institut Henry Dunant, Geneva, 1983; M. Bélanger, *Droit international humanitaire général*, Paris, Gualino, 2007.

[137] M. Safi Youssef, op. cit., pp. 12-15.

as much as possible. IHL is composed of two main branches: the *Geneva Law*, which protects those who are not or no longer taking part in hostilities (e.g., civilians or *hors de combat*); and The *Hague Law*, which regulates the means and methods of warfare (e.g., types of weapons that can be used or the tactics that can be employed). Overarching both branches are the core principles of IHL : distinction, proportionality, and precaution (collectively referred to as the targeting law).

Although AWS intersect with various branches of international law — including international human rights law, international criminal law, the law of the sea, and space law — the most directly implicated framework remains IHL, particularly its sub-branches: weapons law and targeting law. This Chapter undertakes the task of assessing AWS — primarily — under weapons law and under targeting law (Section 2). However, it notes that the applicable legal standards — and consequently, the attribution of responsibility for grave violations of IHL — require a prior qualification of the legal nature of AWS (Section 1). This preliminary step is important because IHL traditionally draws a clear distinction between weapons, which are objects used in warfare, and combatants, who are legal subjects bearing obligations under the law of

armed conflict. Yet, AWS — depending on their level of autonomy — may blur this distinction.

SECTION 1– THE LEGAL NATURE OF AUTONOMOUS WEAPON SYSTEMS

The breadth or narrowness of a state's definition of AWS significantly influences the qualification of their legal nature. For some, AWS encompass existing weapon systems that feature some autonomy in certain functions,[138] for others this category is restricted to systems capable of performing 'cognitive' tasks that mirror human intelligence, meaning they would be able to demonstrate situational awareness, adapt to environment changes, and continuously evolve their capabilities through learning capabilities.[139]

This second perception significantly blurs the lines when it comes to identifying AWS' legal nature: are AWS like any conventional weapon — tools designed and developed in compliance with the weapons law — that are used by human combatants — in compliance with the targeting law — to exert force? Or does the fact that, they select and engage their targets without human intervention, and that arguably their "behavior"

[138] For example: USA, Norway, and ICRC.
[139] For example: France, China and UK.

could be algorithmically programmed to respect IHL principles,[140] enabling them to reliably and consistently distinguish between civilians and combatants, civilian objects and military targets; take all feasible precautions in the attack; and assess the incidental harm to civilian against the expected military advantage, render them closer to combatants than to means of warfare? In such case, the entire framework shifts because IHL regulates weapons and combatants under distinctly different paradigms: a weapon is inherently lawful or unlawful (B), while a combatant may act lawfully or unlawfully (A).[141]

A. THE COMBATANT ANALOGY

The idea that a weapon (robot, machine, or algorithm) could be granted the status of combatant — and thus hold the obligations and bear rights attached to it — might initially be dismissed as illogical. However, it is, in the researcher's view,

---

[140] See notably M. Sassóli, *Autonomous Weapons and International Humanitarian Law: Advantages*, *Open Technical Questions and Legal Issues to be Clarified*, International Law Studies, U.S. Naval War College, Vol. 90, 2014, accessible at: https://digital-commons.usnwc.edu/ils/vol90/iss1/1/.

[141] R. Crootof, *Autonomous Weapon Systems and the Limits of Analogy*, Harvard National Security Journal, Vol. 9, 2018, p. 55, accessible at: https://harvardnsj.org/wp-content/uploads/2018/06/2_Crootof_LimitsOfAnalogy_06.08.18.pdf; see also H.-Y. Liu, *Categorization and Legality of Autonomous and Remote Weapon Systems*, International Review of the Red Cross, Vol. 94, N. 886, 2012, p. 629, accessible at : https://international-review.icrc.org/sites/default/files/irrc-886-liu.pdf

worth consideration. This notion has in fact been examined in legal scholarship, not as an accepted classification, but as part of broader effort to analogize and stretch existing legal categories to include emerging technologies like AWS. Scholars have explored whether such systems, by performing functions traditionally reserved for human combatants, might justify rethinking the boundaries of legal personhood and subjectivity in armed conflict.

In a foundational article titled *Autonomous Weapon Systems and the Limits of Analogy* published in 2018 in the *Harvard National Security Journal*, Rebecca Crootof treated the analogies question in an in-depth manner. She argued and concluded that AWS do not fit neatly into existing legal categories under IHL. Crootof first noted that, in the absence of a dedicated legal regime for AWS, analogical reasoning helps stretch existing law to cover developing technologies and minimize law-free zones.[142] She emphasized that AWS were considered under various potential analogies — namely weapons, combatants, child soldiers, and animal combatants — however, all these analogies fail to address the legal issues

[142] R. Crootof, *The Limits of Analogy*, op. cit., p. 52.

raised by AWS because they "all misrepresent legally salient traits."[143]

Similarly, Hin-Yan Liu argues that the emergence of technologically advanced military platforms challenges traditional understandings of weapons and the 'means and methods of warfare' due to their capacity to filter and analyze information, draw conclusions, and make decisions.[144] He contends that these capabilities set such systems apart from all previous forms of military equipment, positioning them somewhere between the existing legal categories of weapons and combatants. While he does not endorse their classification as combatants, he recognizes that their classification as mere weapons is inadequate.[145]

Tim McFarland observes that, for some, AWS constitute an "artificial substitute for a combatant."[146] This view stems

[143] Ibidem.
[144] H-Y. Liu, op. cit., p. 628.
[145] Ibidem. The author notes that their classification as mere weapons fails both to acknowledge that these systems do not inflict violence in a direct manner but rather serve as intermediary platforms from which weapons are deployed, and to capture their varying levels of autonomy over the use of force. He maintains that regulating AWS solely as weapons "will result, at best, in partial, and therefore inadequate, mechanisms that fail to account for the real challenges that they pose".
[146] T. McFarland, *Autonomous Weapon Systems and The Law of Armed Conflict: Compatibility with International Humanitarian Law,* Cambridge University Press, 2020, p. 67.

from the expectation that future AWS may assume increasingly complex and ambiguous decisions — ones that currently require human involvement. In certain cases, these targeting functions align with legal obligations explicitly assigned to combatants under international law.[147]

Bonnie Docherty recognizes that while "traditional weapons are tools in the hand of a human being, fully autonomous weapons would make their own determinations about the use of force."[148] Similarly, Heather Roff notes that "the weapon is also the combatant, and the decision to target and fire lies with the machine […]."[149]

In the same vein, the previously mentioned report of the former Special Rapporteur Christof Heyns notes that

> LARs are different from earlier revolutions: their deployment would entail not merely an upgrade of the kinds of weapons used, but also a change in the identity of those who use them. With the contemplation of LARs, *the distinction between weapons and warriors risks becoming blurred, as the*

[147] Ibid., p. 73.
[148] B. Docherty, *Shaking the Foundations The Human Rights Implications of Killer Robots*, Human Rights Watch and Harvard Law School International Human Rights Clinic, 2014, p. 5 accessible at: https://www.hrw.org/report/2014/05/12/shaking-foundations/human-rights-implications-killer-robots.
[149] H. Roff, Killing in war: Responsibility, liability, and lethal autonomous robots, in F. Allhoff, N. Evans, and A. Henschke (eds.), *Routledge Handbook of Ethics and War: Just war theory in the 21st century*, Routledge, 2013, pp. 211-212 (cited by T. McFarland and others).

> *former would take autonomous decisions about their own use*.[150]

The previous observations emphasize that AWS, particularly, their potential to operate independently — to select, prioritize, and engage targets without direct human intervention — grants them with attributes traditionally reserved for combatants, such as decision-making on the battlefield. The analogy with combatants, though imperfect, makes sense because these systems are expected to carry out actions that normally require moral judgment, emotional awareness and restraint, or empathy.

Particularly, the plausibility of analogizing AWS to combatants rests on three main factors: first, the way in which AWS are at times discussed as if they bear obligations under IHL[151]; second, their portrayal as lacking the capacity of experiencing human emotions; and third, their inherent inability to be held accountable for acts that would amount to grave violations of IHL.[152]

---

[150] C. Heyns, A/HRC/23/47, op. cit., pp. 5-6. *Italic* added.
[151] HRW, *Losing Humanity*, op. cit., p. 30. The Human Rights Watch (HRW) Report *Losing Humanity: the Case Against Killer Robots* argues that robots would appear to be incapable of abiding by the key principles of international humanitarian law. They would be unable to follow the rules of distinction, proportionality, and military necessity and might contravene the Martens Clause.
[152] T. McFarland, op.cit., pp. 67-69.

AWS are often described as incapable of having human emotions. This point in particular has been equally used by both proponents and opponents of AWS.[153] It was put forward that AWS, due to their lack of human emotions, may be preferable to human soldiers in certain situations or for certain activities. Rebecca Crootof cited a Defense Advanced Research Projects Agency official stating that human beings are becoming "the weakest link in defense systems".[154] In comparison to AWS which "[do not] get hungry, tired, bored, or sick […], tackle the dirty, dangerous, and dull work without complaint […] [and] [do not] act out of fear or anger, for vengeance or vainglory",[155] they could eventually comply with the law of armed conflict

[153] See among others A. Etzioni and O. Etzioni, *Pros and Cons of Autonomous Weapons Systems*, Military Review, 2017, p. 74 ; A. L. Schuller, *At the Crossroads of Control: The Intersection of Artificial Intelligence in Autonomous Weapon Systems with International Humanitarian Law*, Harvard National Security Journal, Vol. 8, 2017, pp. 419-420 ; HRC, *Losing Humanity*, op. cit., p. 4 ; M. Schmitt, *Autonomous Weapon Systems and International Humanitarian Law: A Reply to Critics*, Harvard National Security Journal, Vol. 4, 2013, p. 13; see also, A. Guterres, A/79/88/, op.cit., the submission of Pakistan (p. 85), Serbia (p. 97), and Sri Lanka (p. 104).
[154] R. Crootof, *The Killer Robots Are Here,* op. cit., p. 1867.
[155] Ibidem.; see also, R. Sparrow, *Robots and Respect: Assessing the Case Against Autonomous Weapon Systems*, Ethics & International Affairs, 30, no.1, Cambridge University Press, 2016, p. 97.

better than human soldiers,[156] and can "perform more ethically than human soldiers are capable of".[157]

Conversely, The UN Secretary-General report of 2024 highlights that the use of AWS reduces the opportunity for compassion or moral reasoning in combat situations, especially during complex ethical decisions that require empathy, value judgments or an understanding of human emotions.[158]

The emotion-based arguments, while important for considering the ethical perspectives, also have legal implications. IHL presumes human judgment in its application — particularly when assessing principles like proportionality and precaution. These assessments rely on subjective and context-sensitive evaluations that cannot be reduced to algorithms — even if arguably technically feasible in the future. The inability of AWS to experience or interpret emotions means they lack the intuitive and moral faculties, inherent for human combatants, to deal with ambiguous or morally complex

[156] R. Arkin, Governing *Lethal Behavior in Autonomous Robots*, Chapman and Hall/CRC press, New York, 2009, p. 30, cited by R. Crootof, op. cit., p. 1868.
[157] R. Arkin, *Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/Reactive Robot Architecture*, Technical Report GIT-GVU-07-11, Mobile Robot Laboratory, College of Computing, Georigia Institute of Technology, p. 7, accessible at : https://sites.cc.gatech.edu/ai/robot-lab/online-publications/formalizationv35.pdf.
[158] A. Guterres, A/79/88, op. cit., p. 85.

situations. This absence becomes especially problematic in scenarios involving surrender, wounded combatants, or particularly in scenarios where it is lawful to attack a target, but *immoral* to do so.

For example, Paul Scharre recounts a personal story from when he was serving in the war in Afghanistan in 2004. Scharre and his sniper team were scouting Taliban infiltration routes, when they were spotted by a young girl of five or six years old "ostensibly […] just herding goats," but clearly "spotting for Taliban fighters."[159] According to the story, after the girl left, Taliban fighters arrived, prompting a firefight. Scharre notes that

> Here's the thing: the laws of war don't set an age for combatants. *Behavior determines whether or not a person is a combatant*. If a person is participating in hostilities, as the young girl was doing by spotting for the enemy, then they are a lawful target for engagement. *Killing a civilian who had stumbled across our position would have been a war crime, but it would have been legal to kill the girl*. Of course, it would have been wrong. Morally, if not legally.
> In our discussion, […] [t]he horrifying notion of *shooting a child* in that situation didn't even come up. *We all knew it would have been wrong without needing to say it.* […] *Context is everything. What would a machine have done in our place? It had been programmed to kill lawful enemy combatants; it*

[159] P. Scharre, *Army of None*, op. cit., p. 11.

> *would have attacked the little girl*. Would a robot know when it is lawful to kill, but wrong?[160]

What is notable in this story is that Scharre and his team made a conscious human decision — one that AWS, devoid of emotional and moral cognition, are, in principle, incapable of performing. This inability to exercise context-sensitive and moral judgment, not only weakens the case for considering them as combatants but also, in the researcher's view, diminishes the persuasiveness of proponents' emotion-based arguments — particularly the claim that AWS would avoid atrocities driven by human emotions, such as rape — to justify their deployment.

In addition to the counterargument that AWS could indeed be programmed or deployed in ways that deliberately inflict terror, including through sexual violence — since a machine can be programmed to carry out such acts[161] — it can be argued that the absence of human emotion argument is misplaced in this context. Removing the human element may or may not prevent the occurrence of such atrocities,[162] but if it

---

[160] Ibid., p. 10-11; *Italic* added.

[161] A. Guterres, A/79/88, op. cit., see the submission of Women's International League for Peace and Freedom, p. 176.

[162] C. Carpenter, "*Robot Soldiers Would Never Rape": Un-packing the Myth of the Humanitarian War-Bot,* 2014, accessible at: https://www.duckofminerva.com/2014/05/robot-soldiers-would-never-rape-un-packing-the-myth-of-the-humanitarian-war-bot.html.

does not, and such acts are perpetrated by AWS, it most certainly create an accountability gap. Machines cannot be prosecuted under international criminal law (ICL), and tracing criminal intent (*mens rea*) back to a human operator, commander, or programmer may prove difficult or even impossible to establish beyond a reasonable doubt. This means that, in such cases, the atrocities would have been committed, yet no individual could be held legally responsible or punished.

If the aim is to render warfare "more humane," the solution to unlawful or inhumane conduct is not to automate the battlefield by replacing human combatants with machines or artificial substitutes, under the pretext that robots do not rape, hate, or act out of revenge. Rather, the solution lies in reinforcing human responsibility and compliance with IHL to ensure that war, as a human endeavor, remains constrained by human values.

B. CRIMINAL RESPONSIBILITY

It was previously noted that AWS may functionally act as combatants on the battlefield due to their capacity to decide, target, and engage without human input. However, they are categorically incapable of being treated as such under IHL. Even if one were to argue that they could bear obligations under targeting law, a fundamental question arises: who bears

responsibility when these obligations are violated? Can non-human entities be held *criminally* responsible under ICL?

1. AWS AND CRIMINAL RESPONSIBILITY

In domestic law, some states recognize the criminal liability of non-human entities such as corporations.[163] In such cases, criminal responsibility shifts from its traditional reservation to natural persons to encompass legal persons under certain conditions. But can this logic be extended to AWS? Under ICL, criminal responsibility is inherently tied to the human condition — particularly the attributes of *agency* and *intent*. First, the Rome Statute of the International Criminal Court (ICC Statute) explicitly limits criminal liability to natural persons (human legal entities).[164] Second, it requires not only the commission of a criminal act, but also the existence of *mens rea*, or criminal intent, especially for core crimes such as war crimes, crimes against humanity, and genocide.[165]

---

[163] For example : USA: New York Central & Hudson River Railroad Co. v. United States, 212 U.S. 481, 1909; France: Art. 121-2 of the French Penal Code (Code Pénal); or The Netherlands: Art. 51 of the Dutch Penal Code.

[164] Art. 25 of the Rome Statute states that "1. The Court shall have jurisdiction over natural persons pursuant to this Statute. [...]"

[165] Art. 30 of the Rome Statute states that "1. Unless otherwise provided, a person shall be criminaly responsible and liable for punishment for a crime within the jurisdiction of the Court only if the material elements are committed with intent and knowledge. 2. For the purposes of this article, a person has intent where: (a) In relation to conduct, that person means to

If we momentarily set aside the Rome Statute's limitation to natural persons and imagine that it allows the prosecution of non-human legal entities, we would still face a fundamental obstacle: AWS are not *legal* entities. Unlike states, corporations or international organizations, autonomous weapons do not — at least as of now — possess legal personality. This lack of legal personality renders them incapable of being held accountable before any court of law, let alone the ICC or any *ad hoc* international criminal tribunal. So if an AWS were to violate its so-called "obligations" under IHL and commit grave breaches, who would be sanctioned? It is conceptually incoherent to speak of punishing a machine. Furthermore, it is illogical to accept a robot's imprisonment, disablement, or destruction as a punishment for grave violations of IHL (e.g., directing attacks against civilian populations or directing attacks against buildings dedicated to education or religious practice),[166] neither in the legal sense, not in the purely human sense.

---

engage the conduct; (b) In relation to a consequence, that person means to cause that consequence or is aware that it will occur in the ordinary course of events. [...]"

[166] Art. 8 of the Rome Statute states "2. For the purposes of this Statute, "war crimes" means: (a) Grave breaches of the Geneva Conventions of 12 August 1949, namely any of the following acts against persons or property protected under the provisions of the relevant Geneva Convention: [...] (b) Other serious violations of the laws and customs applicable in international armed conflict, [...] namely, any of the following acts: (i) Intentionally directing attacks against the civilian population as such or against

Beyond legal personality and the inefficacy of punishment as a tool for deterrence or rehabilitation in the case of AWS, the stage of sanctioning seems far-fetched. Even if we imagined an AWS standing trial, it would fail a fundamental precondition for criminal liability: *mens rea*.

The Latin term *mens rea*, literally meaning "guilty mind," refers to the mental state required to be held legally responsible for a crime. The idea of 'guilt' — in our understanding — presupposes moral agency. Moral agency refers to the capacity of an individual to make choices based on an understanding of right and wrong, to weigh consequences, and to act according to ethical principles.[167] Moral agents are expected to regulate their behaviour, not only according to external legal norms, but also according to internal standards (like conscience).[168] Without it,

individual civilians not taking direct part in hostilities; [....] (ix) Intentionally directing attacks against buildings dedicated to religion, education, art, science or charitable purposes, historic monuments, hospitals and places where the sick and wounded are collected, provided they are not military objectives; [...]".

[167] V. Haskar, Moral Agents, in *The Routledge Encyclopedia of Philosophy,* Taylor and Francis, 1998, accessible at: https://www.rep.routledge.com/articles/thematic/moral-agents/v-1.

[168] Ibidem., The author uses the Kantian version of moral agency to explain that, beyond the agent's capacity to conform to the external requirements of morality, it is essential that they should have the capacity to rise above their feelings and passions and act for the sake of the moral law.

a person cannot form the necessary mental state to commit a wrongful act knowingly or intentionally.

The entire structure presupposes that the accused is capable of understanding norms, forming intent, and being rehabilitated or deterred through punishment. Without agency, there can be no intent; without intent there can be no blameworthiness; and without blameworthiness there can be no criminal liability nor punishment. AWS lack agency. They operate based on code, sensors, and pre-defined objectives, and cannot express intent in a meaningful legal or moral sense. Additionally, they do not possess consciousness, self-awareness, or the ability to reflect morally on their actions — nor can they feel guilt, remorse, or shame. Thus, attributing responsibility to AWS disrupts the foundational correlation between criminal justice, blameworthiness, and retribution. It introduces a gap in which no human actor may be directly responsible, yet a grave harm has occurred.

2. RESPONSIBILITY GAP?

If we try to ‘stretch’ the existing responsibility regime to trace responsibility back to the human. Which human would that be? Rebecca Crotoof argues that, in case of use of AWS, the responsibility for the consequences of a decision to use lethal force will no longer be directly traceable to a human operator.

Instead, responsibility may be distributed across multiple actors — including the operator, the military commander, the programmer, the manufacturer, the weapon system itself, or some combination thereof.[169]

In a similar vein, Ann-Katrien Oimann distinguishes between what she calls easy cases and hard cases.[170] Easy cases are those in which a human exploits the system as tool to commit certain crimes — for example, a software engineer who has intentionally programmed a weapon to target civilians, or an operator who deployed the weapon to carry out unlawful attacks. In these cases, the person will be held responsible. In contrast, in hard cases, harm is caused by the AWS, yet no human acted intentionally or carelessly.[171] This is where a responsibility gap emerges.

The notion "responsibility gap" has increasingly been used both in legal scholarship and in states discussions on AWS. However, views diverge on whether such a gap truly exists, or whether it merely reflects challenges in tracing accountability rather than an absence of accountability altogether.[172] Some

[169] R. Crootof, *The Killer Robots Are Here*, op. cit., p. 1845.
[170] A.-K. Oimann, *The Responsibility Gap and LAWS: a Critical Mapping of the Debate,* Philosophy & Technology, vol 36(1), article 3, 2023, p. 3.
[171] Ibidem.
[172] Ibid., p. 7-10.

scholars have proposed new solutions to bridge the gap: for example, Rebecca Crotoof's proposal on "war torts"[173], which suggests imposing strict liability on states for harms caused by autonomous systems, regardless of individual fault; others have explored the possibility of expanding the doctrine of command responsibility to encompass those who deploy or oversee AWS.[174]

This lack of consensus over how to fill the responsibility gap is precisely the reason most states, legal scholars, reports from the ICRC and UN, insist that responsibility must remain with human agents — whether designers, programmers, operators, commanders, or political leaders to ensure accountability under international law.[175] Notably, the notion of

[173] R. Crootof, *War Torts: Accountability for Autonomous Weapons*, University of Pennsylvania Law Review, Vol. 164, No. 6, 2016.

[174] See among others: Y. Guanwan, M-H. Aulawi, R. Anggriawan, and T-A. Putro, *Command responsibility of autonomous weapons under international humanitarian law*, Cogent Social Sciences, vol. 8(1), 2022, accessible at: https://repositori-api.upf.edu/api/core/bitstreams/8460a9ae-6c3a-4db2-91af-5c66f5be3613/content ; D.-J. Posthuma, *Autonomous Weapons Systems and Command Responsibility: Addressing the Specter of Impunity*, Master Thesis, Tilburg University, 2019, accessible at: https://arno.uvt.nl/show.cgi?fid=149083.

[175] See among others: A. Gutteres, A/79/88, op. cit., §23-24; ICRC, *ICRC Position and Background Paper*, op. cit.; ICRC, *Limits on Autonomy in Weapon Systems*, op. cit.; R. Crootof, *War Torts*, op. cit.; V. Boulanin, N. Davison, M. Verbruggen, and N. Goussac, *Limits on Autonomy in Weapon Systems: Identifying Practical Elements of Human Control*, SIPRI and ICRC, 2020.

"meaningful human control" (MHC) has been widely present in discussions over AWS,[176] as a preemptive solution to address this potential gap. Despite variation in phrasing, human control is endorsed by the majority of states.[177]

At its core, MHC refers to ensuring that human judgment and oversight are retained over critical functions of targeting and engagement. However, despite its widespread endorsement, the concept remains difficult to operationalize in practice and there is still no consensus on what degree or type of human involvement is sufficient to qualify as "meaningful" under IHL. Given the breadth of debates surrounding its interpretation and implementation, a comprehensive examination of the concept of MHC falls outside the scope of this study.[178] Nonetheless, its

---

[176] V. Boulanin, N. Davison, M. Verbruggen, and N. Goussac, op. cit., p. 1, footnote 5.

[177] A. Gutteres, A/79/88, op. cit., p. 6, §11-15.

[178] See M. Ekelhof, *Autonomous Weapons: Operationalizing Meaningful Human Control*, ICRC Humanitarian Law & Policy Blog, 2018, accessible at: https://blogs.icrc.org/law-and-policy/2018/08/15/autonomous-weapons-operationalizing-meaningful-human-control/; L. Trabucco, What is Meaningful Human Control, Anyway? Cracking the Code on Autonomous Weapons and Human Judgment, Modern War Institute at West point, 2023, accessible at: https://mwi.westpoint.edu/what-is-meaningful-human-control-anyway-cracking-the-code-on-autonomous-weapons-and-human-judgment/; UNIDIR, *The Interpretation and Application of International Humanitarian Law to Lethal Autonomous Weapon Systems Background paper on the views of States, scholars and other experts*, 2025, accessible at: https://unidir.org/wp-content/uploads/2025/03/UNIDIR_The_Interpretation_and_Application_of_International_Humanitarian_Law_Lethal_Autonomous_Weapon_Syst

relevance to the ongoing regulatory discussions cannot be underestimated: it has emerged as a central legal safeguard for AWS' compliance with IHL.

SECTION 2– THE LEGAL FRAMEWORK(s) GOVERNING AUTONOMOUS WEAPON SYSTEMS

It was previously noted that identifying the legal nature of AWS is a necessary precondition for determining the applicable legal framework. However, their legal qualification — as demonstrated — remains heavily debated: if they cannot be classified as combatants, should they be considered as mere weapons, or do they constitute a distinct category that challenges existing classifications? While there is not yet a clear-cut answer to this question, it directs attention toward existing bodies of IHL to assess whether current frameworks are adequate, or whether new normative instruments are required.

Recognizing the complex challenges posed by AWS, states established a dedicated forum: the Group of Governmental Experts under the Convention on Certain Conventional

ems.pdf; N. Davison, *Autonomous weapon systems: An ethical basis for human control*, ICRC Humanitarian Law & Policy Blog, 2018, accessible at: https://blogs.icrc.org/law-and-policy/2018/04/03/autonomous-weapon-systems-ethical-basis-human-control/.

Weapons. The GGE, a subsidiary body created at the Fifth Review Conference of the CCW in December 2016 pursuant to a decision by the Meeting of High Contracting Parties (HCPs), was tasked with examining the implications of emerging technologies in the area of LAWS.[179] The Group brings together states, legal experts, scientists, civil society and international organizations — not only to discuss the technical, ethical, and military implications of AWS, but also to explore potential pathways for their regulation under international law.

Among the various stakeholders participating at the GGE, different positions exist regarding normative regulation of AWS (A). Many stress the necessity of a legally binding instrument specific to AWS. Conversely, others maintain that the existing legal framework — namely, weapons law (B), targeting law (C) and other relevant IHL rule such as the Martens Clause (D) — is sufficient to govern their development and use. This subsection considers both perspectives. It first explores the different positions on proposed regulatory frameworks and the forms they may take, before turning to IHL as the primary body of law currently applicable to AWS. As reaffirmed in GGE

[179] United Nations, *Final Document of the Fifth Review Conference of the High Contracting Parties to the Convention on Certain Conventional Weapons*, CCW/CONF.V/10, Geneva, 12-16 December 2016, Decision 1, p. 9.

guiding principle (a): "[i]nternational humanitarian law continues to apply fully to all weapon systems, including the potential development and use of lethal autonomous weapons systems."[180]

A. STATES' POSITIONS ON POTENTIAL REGULATORY FRAMEWORKS.

Beyond definitional divergencies, whether or not AWS need to be addressed by a specifically dedicated treaty has been subject for debate among states, institutions, and legal scholars. As of 2025, three main positions exist among states. The first — widely adopted by 129 states and numerous civil society actors — positioned in favor of a new instrument to regulate AWS. The second positioned against a legally binding instrument (12 states). Finally, the third has neither supported nor opposed the idea of regulating them (54 states have not declared any position).[181]

[180] United Nations, *Meeting of the High Contracting Parties to the Convention on Certain Conventional Weapons: Final Report*, *Annex III*: *Guiding Principles affirmed by the Group of Governmental Experts on Emerging Technologies in the Area of Autonomous Weapons System*, CCW/MSP/2019/9, 2019.

[181] Automated Decision Research, *State positions on Autonomous Weapons*, n.d., accessible at : https://automatedresearch.org/state-positions/?_state_position_negotiation=yes.

However, the abstract consideration of these numbers can be misleading. First, among the 129 states supporting a new instrument, divergent standpoints coexist. On the one hand, there are states who support a preemptive ban on fully AWS (e.g., Egypt, Palestine, Austria, Mexico),[182] and on the other hand, there are states that favor the development of regulatory frameworks without necessarily prohibiting them (e.g., China).[183] Additionally, divergent interpretations persist regarding the nature and the structure of the regulatory framework (treaty, principles, practices of responsible use, political declaration, etc.) and the scope of prohibition: should all AWS be banned or should a two-tier approach be considered, banning fully autonomous weapons, while regulating the others?

The "**two-tier approach**,"[184] increasingly supported by actors such as the ICRC and reflected in many state submissions to the Secretary-General and to the GGE, seeks to distinguish between fully autonomous systems that operate without any

[182] A. Guterres, A/79/88, op. cit., p. 42, p. 118, p. 26, and pp. 75-76.
[183] Ibid., pp. 36-37.
[184] Ibid., p. 14 §68 The Secretary-General report notes that "Many States expressed support for the two-tier approach, according to which lethal autonomous weapons systems that could not be used in accordance with international law should be prohibited, while others should be appropriately regulated. [...]".

meaningful human control, and other types of AWS that retain some form of human oversight. Under this approach, the development, and use of fully autonomous weapons would be explicitly prohibited, while AWS that incorporate sufficient human control would be subject to regulation and compliance with IHL.[185]

Despite this increasing agreement on the necessity of prohibiting AWS that cannot comply with IHL, the result remains an absence of an international treaty or a mandate to negotiate one within the CCW framework, largely due to the consensus-based nature of the forum and the resistance of a few

[185] Ibid., p. 29. Bulgaria notes that "[t]he two-tier approach calls for a distinction between (a) autonomous weapons systems operating completely outside human control and a responsible chain of command; and (b) autonomous weapons systems featuring autonomous functions, requiring regulations to ensure compliance with international law and, more specifically international humanitarian law"; p. 43 "Egypt is of the view that pursing a two-tiered approach comprising the prohibition of fully autonomous weapons and the regulation of other military applications of artificial intelligence represents the most realistic and effective course of action"; p. 64 Italy notes that "Although not facing a legal vacuum, in Italy's view a normative and operational framework [...] needs to be further developed. This could be done using a two-tier approach for setting prohibitions and regulations. According to this approach, lethal autonomous weapons systems that cannot be developed and used in accordance with international humanitarian law would be ipso facto prohibited. On the other hand, systems featuring decision-making autonomy in critical functions, which can be developed and used in full compliance with international humanitarian law, would be regulated", among other examples.

key states. Nonetheless, in December 2023, the United Nations General Assembly adopted its first Resolution on LAWS A/RES/78/241, which calls for accelerated international efforts toward the regulation of AWS.[186] In the same vein, the UN Secretary-General explicitly urged states to conclude a treaty on LAWS by 2026.[187]

Regardless of the likelihood of such treaty being effectively concluded, states reached consensus in 2018 on the adoption of 11 guiding principles on AWS, which continue to shape the ongoing normative debate.[188] These principles are:

> a) International humanitarian law continues to apply fully to all weapons systems, including the potential development and use of lethal autonomous weapons systems;
> (b) Human responsibility for decisions on the use of weapons systems must be retained since accountability cannot be transferred to machines. This should be considered across the entire life cycle of the weapons system;
> (c) 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,

[186] United Nations General Assembly, *Resolution 78/241: Lethal Autonomous Weapons Systems,* A/RES/78/241, adopted on 22 December 2023, accessible at: https://docs.un.org/en/A/RES/78/241.
[187] A. Guterres, A/79/88, op. cit., p. 18, §90.
[188] GGE, CCW/MSP/2019/9, op. cit.

a range of factors should be considered including the operational context, and the characteristics and capabilities of the weapons system as a whole;
(d) 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, including through the operation of such systems within a responsible chain of human command and control;
(e) In accordance with States' obligations under international law, in the study, development, acquisition, or adoption of a new weapon, means or method of warfare, determination must be made whether its employment would, in some or all circumstances, be prohibited by international law;
(f) When developing or acquiring new weapon systems based on emerging technologies in the area of lethal autonomous weapons systems, physical security, appropriate non-physical safeguards (including cyber-security against hacking or data spoofing), the risk of acquisition by terrorist groups and the risk of proliferation should be considered;
(g) Risk assessments and mitigation measures should be part of the design, development, testing and deployment cycle of emerging technologies in any weapons systems;
(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;
(i) In crafting potential policy measures, emerging technologies in the area of lethal autonomous weapons systems should not be anthropomorphized;
(j) technologies; 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

> (k) The CCW offers an appropriate framework for dealing with the issue of emerging technologies in the area of lethal autonomous weapons systems within the context of the objectives and purposes of the Convention, which seeks to strike a balance between military necessity and humanitarian considerations.[189]

Although non-binding, the 11 guiding principles constitute a form of soft law that reflects a degree of consensus around core aspects of AWS, bridging the existing legal obligations and potential future regulatory initiatives. Notably, principle (a) reiterates that IHL continues to apply fully to all weapon systems, including AWS. Equally, critical are principles (b), (c), and (d), which insist on the retention of human responsibility and the need for a responsible chain of command-and-control over these systems. They reaffirm that machines, regardless of their level of autonomy or sophistication cannot assume legal accountability. Principle (e) further links this obligation to the established rule of weapons reviews under IHL, specifically under Article 36 of AP I to the Geneva Conventions.

Under current legal frameworks, AWS are required to comply with two sets of IHL rules : the weapons law and the targeting law. First, they need to be assessed for legality under the weapons law (control in design and development) to

[189] Ibidem.

determine whether their development or acquisition would be unlawful *per se*. If this is not the case, then their use needs to be assessed for compliance with the principles of distinction, proportionality, and precaution under the targeting law (control in use). In simpler terms, the weapon itself needs to first be 'cleared' to be used in battlefields. Once deployed in battlefields, its use for targeting and engaging becomes constrained by the core principles of IHL.

B. WEAPONS LAW

Weapons law is a branch of IHL that governs the legality of the means of warfare — i.e., the tools used to inflict harm during armed conflict.

1. GENERAL PROHIBITIONS

The central premise of weapons law is codified in Article 35 (1) of AP I to the Geneva Conventions, which provides that in any armed conflict, "the right of the Parties to the conflict to choose methods or means of warfare is not unlimited."[190] This general prohibition is expanded in paragraphs (2) and (3) of the same article, which respectively ban weapons that cause

[190] This principle is stipulated in Article 35 (1) of AP I and in Article 22 of the 1907 Hague Regulations Respecting the Laws and Customs of War on Land : "The right of belligerents to adopt means of injuring the enemy is not unlimited".

superfluous injury or unnecessary suffering, and those intended or expected to cause widespread, long-term, and severe damage to the natural environment.[191] This rule is relevant if the AWS were specifically designed to cause damage to the natural environment which would render it unlawful *per se*.

However, these rules cannot be considered in isolation from another fundamental prohibition under IHL: the weapon system must not be indiscriminate by nature. Article 51(4) of AP I explicitly prohibits indiscriminate attacks, defined as attacks not directed at a specific military objective, or those which employ a method or means of combat which cannot be directed at specific military objective, or whose effects cannot be limited as required by IHL.[192]

This prohibition implies that any weapon which, by its nature, cannot be directed solely at military objectives or whose

[191] Art. 35: (2) It is prohibited to employ weapons, projectiles and material and methods of warfare of nature to cause superfluous injury or unnecessary suffering. (3) It is prohibited to employ methods and means of warfare which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment.

[192] Article 51 (4) of AP I : "Indiscriminate attacks are prohibited. Indiscriminate attacks are: (a) those which are not directed at a specific military objective; those which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction".

effects cannot be contained to avoid excessive civilian harm is unlawful *per se*. The ICRC's Customary IHL Study confirms the customary status of these general prohibitions.[193] Notably, they apply regardless of whether a state is party to AP I.

In the context of AWS, these prohibitions require assessing whether a weapon is capable of complying with the principle of distinction and can only be aimed at lawful military targets. Many critics argue that AWS, by their very nature, might be incapable of consistent distinction or proportionality, effectively making them inherently indiscriminate by nature and thus unlawful *per se*.[194] However, from a legal standpoint, whether AWS are inherently indiscriminate is a matter of technical assessment: a well-designed autonomous system could, in theory, select lawful targets with greater precision than a human, whereas a poorly designed one might not. In this regard, Neil Davison, an adviser at Arms Unit of the ICRC observes that determining the lawfulness of an AWS will "depend on its specific characteristics and whether, given those characteristics, it can be employed in conformity with the rules of IHL in all the

[193] ICRC, *Rule 70: Weapons of a Nature to Cause Superfluous Injury or Unnecessary Suffering* and *Rule 71: Weapons That Are by Nature Indiscriminate*, in Customary IHL Database, accessible at: https://ihl-databases.icrc.org/en/customary-ihl.
[194] V. Boulanin and M. Verbruggen, op. cit., p. 47.

circumstances in which it is intended and expected to be used".[195] Similarly, any weapon specifically designed to cause superfluous injury on unnecessary suffering would be unlawful *per se*. The unlawfulness also extends if the system is used as a platform from which to use weapons that are prohibited under IHL (e.g., blinding laser, undetectable fragments, biological agents, etc.).

2. TREATY-BASED PROHIBITIONS

In addition to these general prohibitions, weapons law encompasses treaty-based prohibitions on specific weapon types. Treaties like the Biological Weapons Convention,[196] the Chemical Weapons Convention,[197] the Ottawa Convention on anti-personnel landmines,[198] or the Oslo Convention on cluster munitions,[199] among others, were negotiated to ban or restrict

[195] N. Davison, *A legal perspective: Autonomous weapon systems under international humanitarian law*, UNODA Occasional Papers, No. 30, United Nations Office for Disarmament Affairs, 2018, p. 9.
[196] Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction of 1972 (entered into force 26 March 1975).
[197] Convention on the the Prohibition of the Development, Production and Stockpiling and Use of Chemical Weapons and on their Destruction of 1993 (entered into force 29 April 1997).
[198] Convention on the the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction of 1997 (entered into force 1 March 1999).
[199] Convention on Cluster Munitions of 2008 (entered into force 1 August 2010).

certain weapons that are deemed operationally uncontrollable under IHL or morally unacceptable. While not directly relevant to AWS, which are defined by their mode of operation (autonomy) rather than by the specific agent or munition involved, they can be relevant if, for example, an AWS used a chemical agent or a biological agent as its means of harm. It would therefore fall under those treaties.

Other than the previously mentioned treaties, the CCW of 1980 is recognized by states, as the most relevant framework in the context of AWS.[200] The CCW is a general umbrella convention under which states have negotiated specific protocols banning or restricting particular weapons deemed to cause unnecessary suffering or to be indiscriminate (e.g., Protocol III on incendiary weapons, or Protocol IV on blinding laser weapons). Discussions on AWS — particularly since 2021 — have been framed in terms of whether or not to negotiate a sixth Protocol to the CCW to ban lethal AWS that lack meaningful human control and to regulate all others.[201]

---

[200] A. Guterres, A/79/88, op. cit., p. 12 §51.

[201] Ibid., p. 13 §58; see also submissions of Bulgaria (p.29 et s.), Ibero-American countries (p. 20), Chile, Colomia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Kazakhstan, Nigeria,, Panama, Peru, Philippines, Sierra Leone and State of Palestine (p. 34), France (p. 49), Germany (p. 52), Italy (p. 63), Luxembourg (p. 73), The Netherlands (p. 77), Norway (p. 82), among others.

However, the CCW's consensus requirement meant that, with persistent disagreement, states could only agree to continue discussions, but not to launch negotiations on a new protocol. Even though no treaty explicitly addresses them, AWS do not exist in a legal vacuum. They remain regulated by general IHL and customary law, and states are bound to ensure that any use of AWS complies with IHL, particularly the requirements enshrined in Article 35 of AP I. One practical mechanism to enforce these requirements is the obligation to conduct legal reviews of new weapons enshrined in Article 36 of the same protocol.

3. LEGAL REVIEW

Reviewing the legality of new weapons is not a novel concept, it dates back to 1868 particularly to the St. Petersburg Declaration which addresses the development of future weapons in these terms:

> The Contracting or Acceding Parties reserve to themselves to come hereafter to an understanding whenever a precise proposition shall be drawn up in view of future improvements which science may affect in the armament of troops, in order to maintain the principles which they have established, and to conciliate the necessities of war with the laws of humanity.[202]

[202] ICRC, *Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight*, 29 November / 11 December

Today, this obligation is explicitly stipulated in Article 36 of AP I which states:

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

It applies to :

> • weapons of all types weapons of all types — be they anti-personnel or anti-materiel, "lethal", "non-lethal" or "less lethal"- and weapons systems;
> • the ways in which these weapons are to be used pursuant to military doctrine, tactics, rules of engagement, operating procedures and countermeasures; […].[203]

In addition to its broad material scope, the ICRC's *Guide to the Legal Review of New Weapons* emphasizes that this obligation applies to all states, regardless of whether or not they are party to AP I.[204] According to the ICRC, the faithful and responsible application of international law requires a state to

1868, accessible at: https://ihl-databases.icrc.org/en/ihl-treaties/st-petersburg-decl-1868/declaration?activeTab=.

[203] ICRC, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measure to Implement Article 36 of Additional Protocol I of 1977*, Geneva, 2006, p. 9, accessible at: https://www.icrc.org/en/publication/0902-guide-legal-review-new-weapons-means-and-methods-warfare-measures-implement-article.

[204] Ibid., p. 4.

ensure that the new weapons it develops or acquires will not violate its international law obligations.[205]

Particularly in the context of AWS, this obligation requires a prior understanding of what these weapons are — not only in conceptual or definitional terms, but also in practical, operational ones. AWS are 'systems' rather than discrete weapons, meaning they integrate sensors, algorithms, control systems, communication systems, and lethal effectors. This systemic nature of their functionality cannot be overlooked in the review process; nor can the obligation be limited to evaluating the weapon in isolation. Rather, the entire architecture relies on the use of autonomy to support the targeting process, which necessitates a complex assessment to ensure that any attack occurs in conformity with the fundamental rules and principles governing the conduct of hostilities.[206] Therefore, for an AWS to pass the legal review and be considered lawful, it must be capable of adhering to the rules of distinction, proportionality, and precaution in attack.[207]

In this regard, a legal review, as mandated under Article 36, cannot meaningfully assess an autonomous weapon's lawfulness without examining the underlying technologies that

[205] Ibidem.
[206] V. Boulanin and M. Verbruggen, op. cit., p. 73.
[207] Ibidem.

make it capable of complying with IHL principles — and their limitations. Whether AWS can in fact demonstrate such capacity remains highly debated, especially given that fully AWS have not yet been widely reported as operational. Nevertheless, what is certain is that their review necessitates multidisciplinary teams composed of legal experts, engineers, military operators, and ethicists to ensure that the process remains robust and thorough.

Moreover, an additional challenge arises: the legality assessment cannot be confined solely to the development phase, particularly for weapon systems with in-field learning capabilities as they "can nullify the weapons testing verification and validation over time".[208] This concern is especially notable for weapons relying on machine learning — a subtype of AI that evolves over time from its original software programming, and that can adapt its programming during deployment. Consequently, reviewing such systems requires mechanisms for post-deployment monitoring, recognizing that system

[208] A. B. Fisher, *How international humanitarian law will constrain the use of autonomous weapon systems in the conduct of hostilities*, Masters Thesis, Murdoch University, 2022, p. 50, accessible at: https://researchportal.murdoch.edu.au/esploro/outputs/graduate/How-international-humanitarian-law-will-constrain/991005542029107891/filesAndLinks?index=0

behaviour may evolve or adapt in ways unforeseen at the moment of review.

Furthermore, ensuring compliance at the design phase poses serious challenges for programmers and developers. It would require the capacity to translate IHL obligations into mathematical equations and code — a task that can be significantly difficult, especially when assessing proportionality or distinction in ambiguous situations. For example, identifying a combatant rendered *hors de combat* without any visible changes in their physical attire, or determining whether a civilian is 'directly participating in hostilities — particularly given the lack of consensus on the meaning of direct participation[209] — are challenging tasks for human soldiers; one can only imagine how they would be performed by a machine lacking contextual understanding or the capacity to exercise moral judgment. These examples, and others, legitimately raise several questions about the actual technical feasibility of

[209] Neither the Geneva Conventions nor their Additional Protocols provide a definition of what activities amount to direct participation in hostilities. For more on the notion of direct participation see : ICRC, *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*, Geneva, 2009, accessible at: https://www.icrc.org/en/publication/0990-interpretive-guidance-notion-direct-participation-hostilities-under-international; E. Christensen, *The Dilemma of Direct Participation in Hostilities*, Florida State University Journal of Transnational Law & Policy, Vol. 19, Issue 2, Article 2, 2010, accessible at: https://ir.law.fsu.edu/jtlp/vol19/iss2/2/.

creating fully AWS that can — predictably and reliably — undertake these context-sensitive judgments without incorporating General AI (GAI).[210]

C. TARGETING LAW

Once a weapon has been determined to be lawful *per se* under weapons law, its use must comply with the rules governing the conduct of hostilities. This set of rules, commonly referred to as targeting law, governs how any weapon or tactic must be used in armed conflict. The core targeting principles are: distinction, proportionality, and precautions in attack, and are enshrined in AP I — notably Articles 48, 51, 52, 57. These rules are universally authoritative, even for states that are not parties to AP I, as they are widely recognized as customary international law binding on all states and parties to conflict.[211]

However, it should be noted that there is no consensus among states, institutions, nor legal scholars regarding the (non)compliance of AWS with these principles. In fact, this remains one of the most active areas of debate today. Many hold the view that AWS cannot comply with the core principles of

[210] See Chapter 3–Section 1 for a distinction between different types of AI.
[211] ICRC, *Rule 1: The Principle of Distinction between Civilians and Combatants*, *Rule 14: Proportionality in Attack*, and *Rule 15: Precautions in Attack*, in Customary IHL Database, accessible at: https://ihl-databases.icrc.org/en/customary-ihl.

IHL,[212] or — on a different but related note — that they breach the Martens Clause.[213] Conversely, others argue that AWS can indeed comply with the core principles of IHL, or claim that AWS could achieve better compliance with IHL principles than human operators.[214]

These divergent viewpoints underscore the complexity of assessing AWS' compliance with targeting law, particularly given that such weapons remain, for now, largely conceptual. It appears then that their assessment should be made on a case-by-case basis rather than categorically, since such compliance depends on three variables: technical feasibility, the complexity of the environment of deployment, and the nature of the assigned task.

At this point, to meaningfully examine their compatibility with IHL, it is necessary to move beyond the broad definitional

[212] C. Heyns, A/HRC/23/47, op. cit., p. 13 §67; HRW, *Losing Humanity*, op. cit., pp. 30-34; A. Guterres, A/79/88, op. cit., p. 8 §23; and E. Winter, *The Compatibility of Autonomous Weapons with the Principles of International Humanitarian Law*, Journal of Conflict & Security Law, Oxford University Press, 2022, pp. 3-5.

[213] R. Sparrow, *Ethics as a source of law: The Martens clause and autonomous weapons*, ICRC Humanitarian Law & Policy Blog, 2017, accessible at: https://blogs.icrc.org/law-and-policy/2017/11/14/ethics-source-law-martens-clause-autonomous-weapons/ ; HRW, *Losing Humanity*, op. cit., pp. 35-36; A. Guterres, A/79/88, op. cit., p.9 §27, submission of Sri Lanka (p. 104) and HRW submission (p.145).

[214] E. Winter, op.cit., p. 2 and pp. 6-7 ; M. Schmitt, op. cit., p. 25.

debates surrounding AWS and specify that the following analysis will concern itself exclusively with "fully" AWS — i.e., those that function entirely autonomously, without human intervention, throughout the OODA loop. These are the systems that will be required to uphold the core IHL principles when in use, without direct real-time human input, beyond activation.

1. THE PRINCIPLE OF DISTINCTION

Codified in Article 48 of AP I, the principle of distinction requires that parties to a conflict distinguish *at all times* between civilians and combatants, and between civilian objects and military objectives. Attacks may only be directed against military objectives and combatants. Article 51(2) further affirms the absolute prohibition of targeting civilians. This is echoed in Rule 1 of the ICRC's Customary IHL Study, which qualifies distinction as a norm of customary international law applicable in both international and non-international armed conflicts.[215]

As the ICRC emphasizes, those who plan decide upon and carry out an attack must ensure that the weapon and the way it is used permit compliance with distinction.[216] Any AWS, to be lawfully used, must be capable of applying this discrimination

[215] See ICRC, *Rule 1. The Principle of Distinction between Civilians and Combatants*, op.cit. : https://ihl-databases.icrc.org/en/customary-ihl/v1/rule1.
[216] N. Davison, op. cit., p. 7.

in target selection. In practice, this means the system's sensors, algorithms, and targeting criteria must reliably identify valid targets (e.g., enemy combatants, military vehicles, military installations, etc.) and avoid non-targets (e.g., civilians, civilian objects, *hors de combat* persons).

This raises a preliminary concern whether a machine can — at all times — adequately interpret complex combat contexts to avoid mistakes in targeting. For example, can an autonomous drone distinguish a combatant picking up another wounded comrade from a civilian aiding an injured person? Can it recognize surrender or other signs of *hors de combat* status? These are difficult problems for artificial vision and pattern recognition.[217] If an AWS cannot be trusted to reliably distinguish, deploying it would amount to inherently indiscriminate attacks, violating IHL.

Despite that, some proponents argue that advanced AI could eventually surpass human targeting accuracy[218] — for instance, by processing sensor data faster without the stress and confusion soldiers face — theoretically reducing targeting errors and enhancing compliance with the principle of distinction.

[217] ICRC, *Autonomous weapon systems: Technical, military, legal and humanitarian aspects*, Expert meeting, Geneva, 26-28 March 2014, p. 12.
[218] See E. Winter, op. cit., pp. 6-7 and pp. 18-19; M. Schmitt, op. cit., pp. 12-13.

However, to date, these remain aspirations, lacking sufficient operational proof.[219] The core challenge thus becomes whether, in the actual state of technology, a machine can consistently and reliably distinguish between lawful and unlawful targets, especially in dynamic or complex environments.

The SIPRI report provides insight. It underscores the limitations of existing Automated Target Recognition (ATR) systems, which can only recognize targets that match pre-defined criteria. Meaning that if these systems can — to a certain extent — comply with the principle of distinction, they can only do so in a basic manner, without any understanding of the context or environment. Their method is rudimentary: they disregard anything that does not correspond to the predefined target profile.[220]

Importantly, they are incapable of assessing the presence of civilians or civilian objects around the target — a foundamental requirement to the application of the principles of proportionality and precaution.[221] These technical limitations are compounded by evolving battlefield realities — e.g., combatants who do not wear uniforms, the presence of human

[219] V. Boulanin and M. Verbruggen, op. cit., pp. 24-26.
[220] Ibidem.
[221] Ibidem.

shields, or dual-use objects — all of which require situational understanding and interpretation.[222]

In light of these challenges, the ICRC has rightly suggested that operational constraints — such as limiting AWS deployment to environments devoid of civilians, restricting their use to targeting material military objectives, or requiring continuous human supervision — may be necessary mitigation measures to uphold the distinction principle in practice.[223]

Assuming that an AWS could meet the threshold of distinction, its compliance with IHL cannot be presumed solely on that basis. The principles of proportionality and precaution in the attack are equally critical. They impose additional obligations that are both fact-specific and context-sensitive — obligations that cannot be satisfied by sensors and algorithms alone and that require nuanced human judgment.

2. THE PRINCIPLE OF PROPORTIONALITY

Codified in Article 51(5) (b) of AP I and reflected in Rule 14 of the ICRC'S Customary IHL Study, the principle of proportionality prohibits attacks that "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be

[222] HRW, *Losing Humanity*, op. cit., pp. 30-32.
[223] ICRC, *ICRC Position On Autonomous Weapon Systems*, op. cit., p. 10.

excessive in relation to the concrete and direct military advantage anticipated."[224] In simple words, while some collateral damage is permissible under IHL, it cannot be disproportionate to the anticipated military advantage.

Traditionally, this assessment is conducted by a human commander or an operator before an attack.[225] But when an AWS is tasked with selecting targets and initiating attacks independently, a critical question arises: who performs the proportionality analysis? And more fundamentally, can 'military advantage' be quantified for an AI-enabled weapon system to assess? How can 'humanity' be mathematically represented? How are civilian lives and property valued in such calculations? These cannot be reduced to merely computational processes — they are moral and legal judgments, that involve complex reasoning that today's AI cannot reliably replicate.

Maciek Zając notes that AWS compliance with the principle of proportionality is widely seen as one of the hardest ethical and legal challenges.[226] He breaks down the principle of

[224] ICRC, *Practice relating to Rule 14. Proportionality in Attack*, accessible at: https://ihl-databases.icrc.org/en/customary-ihl/v2/rule14.
[225] N. Davsion, op. cit., p. 7.
[226] M. Zając, *AWS compliance with the ethical principle of proportionality: Three possible solutions*, Ethics and Information Technology, Vol. 25, article 13, 2023, p. 1, accessible at: https://link.springer.com/article/10.1007/s10676-023-09689-8.

proportionality into a three-part test : (1) Collateral Damage Estimation (CDE), (2) Anticipated Military Advantage (AMA), and (3) Determination of Excessiveness;[227] and stresses these steps are separable and can, theoretically, be divided between human agents and machines.[228]

Regarding the CDE, Zając argues they are feasible to automate through software since it involves physics-based predictions rather than ethical reasoning.[229] In the same vein, Michael Schmitt and Elliot Winter propose the adaptation of Collateral Damage Estimation Methodologies (CDEMs) to enable AWS to perform proportionality assessments.[230] CDEMs are systemic, military-developed procedures for estimating potential collateral damage likely to result from an attack on a given target.[231] For example, the United States military employs a multi-stage CDEM process analyzing factors such as: the area of effect of different weapon types, the blast radius and explosive yield, civilian demographics in the target area and likelihood of civilian presence, structural composition of nearby building, or the timing of the attack.[232]

---

[227] Ibid., pp. 3-7.
[228] Ibid., p. 1.
[229] Ibid., p. 3.
[230] E. Winter, op. cit., pp. 16-17 ; M. Schmitt, op. cit., pp. 19-20.
[231] E. Winter, p. 16; M. Schmitt, p. 19.
[232] E. Winter, op. cit., p.16.

Through these factors, a CDEM generates an estimate of how many civilians and which objects might be harmed if a strike is carried out. Schmitt suggests AWS might, in theory, generate results no less reliable than existing CDEMs operated by human commanders, given that CDEMs rely heavily on algorithms and data modeling.[233] However, the author recognizes a critical limitation: while AWS might process collateral harm estimates, they are less suited to evaluate the other side of the equation — the anticipated military advantage.[234] In other words, while an AWS might replicate the quantitative side of the proportionality equation, they remain ill-equipped to evaluate the qualitative element — the anticipated military advantage — which is highly context-dependent and often requires subjective judgment.

This brings us to the second part of the proportionality test: AMA. It is first important to note that CDEMs are not legal determinations of proportionality, rather they are used to decide the level of command authority required to approve a strike: the higher the estimated collateral damage, the higher the rank needed for authorization.[235] This is because assessing what military gain is expected is inherently contextual and resistant

[233] M. Schmitt, op. cit., p. 20.
[234] Ibidem.
[235] Ibid., pp. 19-20.

to quantification; it demands judgments about strategic and tactical significance that vary across operational levels and are often shaped by subjective assessments of commanders.[236] As Zając explains, that as stipulated by Rule 14 and AP I, AMA must be "concrete and direct", yet even experienced human actors struggle to link tactical actions with higher-level objectives in real-time, which renders attempts to pre-code such assessments into AWS complicated.[237] Moreover, proportionality assessments are not static or one time calculations but are revisited as the battlefield conditions evolve.

Finally, the determination of excessiveness, which integrates CDE and AMA, represents the most abstract and subjective part of the test. Zając identifies this as "the core of the principle of proportionality, as well as the source of the most intractable problem it poses"[238] because it involves comparing "contradictory and dissimilar values with no common metric."[239] In simpler terms, excessiveness requires balancing

[236] M. Zając, pp. 3-4.
[237] Ibid., p .4.
[238] Ibid., p. 5.
[239] M. Homayounnejad, *Lethal Autonomous Weapon Systems Under the Law of Armed Conflict*, PhD Thesis, King's College London, 2018, p. 244, accessible at: https://kclpure.kcl.ac.uk/ws/portalfiles/portal/110384075/2019_Homayounnejad_Maziar_0222601_ethesis.pdf.

fundamentally different kinds of values without a shared measure of comparison.

Elliot Winter proposes that a system could be developed allowing a "like-for-like" numerical comparison.[240] The aim is to turn the proportionality balancing between collateral harm and military advantage into a calculable equation.[241] Yet, he conceded that this would likely require advances in high-level AI, that in experts' estimates are not achievable before 2040 and maybe even 2062.[242] Similarly, Zając recognizes that this layer requires "metacognitive thinking", beyond the current or foreseeable cognitive capacities of AI.[243]

To address these challenges, Zając proposes three solutions to enable AWS compliance with proportionality. The first solution limits AWS operations to civilian-free or minimally populated zones (e.g., naval warfare, certain air operations), thereby eliminating the need for proportionality analysis in many scenarios since collateral harm is improbable.[244] The second involves human commanders conducting proportionality assessments in advance for specific high-value

[240] E. Winter, op. cit., p. 17.
[241] Ibidem.
[242] Ibid., p. 15.
[243] M. Zając, op. cit., pp. 6-7.
[244] Ibid., pp. 7-8 and p. 12.

targets, with AWS executing pre-authorized strikes within tightly defined spatio-temporal parameters, replicating current practices for manned targeted strikes.[245] The third — more controversial — approach entails commanders assigning collateral damage "price tags" to categories of targets (e.g., tanks, artillery), pre-determining permissible collateral harm levels that AWS must not exceed, based on static AMA assumptions.[246]

The proposed solutions may theoretically ensure a system's compliance with the proportionality principle, however, operational realities suggest otherwise. For instance, the use of "price tags" assigned to categories of targets solution, has proven particularly problematic when applied to human targets.[247] In this light, the responsibility for insuring compliance with the principle of proportionality cannot at least for the time being — be fully delegated to an algorithm. It remains the responsibility for human commanders and operators to guarantee that AWS are employed in a manner consistent with IHL. This leads again to the critical role of meaningful

[245] Ibid., p. 8.
[246] Ibid., pp. 10-12.
[247] See Chapter 3–Section 2: AWS in recent armed conflicts, case-study nº. 4: the armed conflict in Gaza.

human control as a normative requirement to uphold moral and legal accountability over decisions of the use of force.

3. THE PRINCIPLE OF PRECAUTION

Codified in Article 57 of AP I and reflected in Rule 15 of the ICRC's Customary IHL Study, the principle of precaution represents a point of intersection between the principles of distinction, proportionality, and humanity. The article stipulates that

> 1. In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects.
> 2. With respect to attacks, the following precautions shall be taken:
> (a) those who plan or decide upon an attack shall:
> (i) do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives within the meaning of paragraph 2 of Article 52 and that it is not prohibited by the provisions of this Protocol to attack them;
> (ii) 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;
> (iii) refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated;
> (b) an attack shall be cancelled or suspended if it becomes apparent that the objective is not a military

> one or is subject to special protection or that the attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated;
> (c) effective advance warning shall be given of attacks which may affect the civilian population, unless circumstances do not permit.
> 3. 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. […].

Article 57 (1) requires parties to a conflict to exercise "constant care" to spare civilians and civilian objects throughout military operations. This obligation is overarching and extends beyond the immediate act of attack, imposing a continuous and proactive duty on military planners and decision-makers during the conduct of military operations.[248]

Maziar Homayounnejad highlights two important observations regarding this requirement. First, although the term constant care is not explicitly defined, it clearly entails a recurring obligation. It is therefore not sufficent to exercise caution only during pre-deployment phases while disregarding

[248] M. Homayounnejad, op. cit., pp. 252-253; E.T. Jensen, *Autonomy and Precautions in the Law of Armed Conflict*, International Law Studies, vol. 96, 2020, pp. 586-587, accessible at: https://digital-commons.usnwc.edu/ils/vol96/iss1/19/.

evolving risks to civilians after a lethal autonomous weapon has been launched. Second, he notes that the obligation applies broadly to all aspects of military operations, not solely to the conduct of specific attacks.[249] This makes constant care a pervasive obligation, which is incumbent upon all persons who have control over the use and deployment of AWS.[250]

Article 57(2) provides examples of this obligation's practical application in the specific context of the attack. It entails four duties that must be respected by those who plan or decide upon an attack: target verification; choice of means and methods; refraining from launching attacks that would result in "excessive" incidental harm in relation to military advantage anticipated; and canceling or suspending an attack if the status of the target shifts to unlawful military target, or if the attack would result in excessive incidental harm.

Paragraph (2), in particular, is where the overlap with the principles of distinction and proportionality materializes. Precautionary measures bridge the rules on distinction and proportionality. At their essence, they are the practical manifestations of balancing military necessity with the principle of humanity, and is where the legal principles are translated into

[249] M. Homayounnejad, op. cit., p. 266.
[250] Ibidem.

operational decisions. As such, they are foundational for the application of proportionality. Maciek Zając explains that the proportionality assessments are only necessary when (1) there are civilians and civilian objects close enough to the attack's military objective to make collateral damage a possibility, and (2) when precautionary measures fail to eliminate the possibility of collateral damage.[251] This renders precaution the practical mechanism that enables the principles of distinction and proportionality to function on the ground.

First, Article 57(2)(a)(i) of AP I imposes an obligation to do everything possible to verify that targets are lawful military objectives and not civilians or civilian objects. It is framed as an obligation of conduct, not of result — i.e., compliance depends on due diligence and "what is practicable or practically possible" given the circumstances at the time, including military necessity and humanitarian considerations.[252] The feasibility of such verifications by AWS remains contested as it is contingent on developments in ATR technology, sensors reliability and the sophistication of the control system.

Nevertheless, some scholars are of the view that AWS may render certain precautions, which would not be available to

[251] M. Zając, op. cit., p. 7.
[252] M. Homayounnejad, op. cit., pp. 253-254.

a soldier, feasible[253] — particularly by extending verification capacity through advanced sensors and data processing. Yet, this potential is dependent on the system's design and battlefield context, something that the current limitations in technology, render challenging — if not impossible — at least in "all" circumstances.

Second, article 57(2)(a)(ii) imposes an obligation on attackers to take all feasible precautions in the choice of means and methods of attack to minimize incidental civilian harm. This obligation is particularly relevant when the commander makes the choice to deploy an AWS, as its deployment may arguably in itself represent a precautionary measure.[254]

Simultaneously, it raises the question of whether the use of AWS can transform in the future into a legal obligation under IHL. In this regard, Marc Sassóli argues that if autonomous systems demonstrate greater reliability than human operators in taking precautions, and if such systems are available in the arsenal without being reserved for higher-risk or higher-priority tasks, then states and commanders are under an obligation to use them.[255]

---

[253] M. Sassóli, op. cit., p. 336.
[254] M. Homayounnejad, op. cit., p. 233.
[255] M. Sassóli, op. cit., p. 320; the author notes that "if autonomous systems are better than human beings, such as in taking precautions, and a State

In the same vein, Homayounnejad maintains that AWS should not be deployed if alternative weapon systems capable of causing less expected collateral damage are available for achieving the same anticipated military advantage. Conversely, if the use of an AWS is likely to reduce collateral harm in a given operational context, and remains a feasible option, then Article 57(2)(a)(ii) may impose a positive obligation to deploy it.[256]

Additionally, proponents of AWS argue that such systems have the potential to discharge means-based precaution better than human combatants.[257] Elliot Winter argues that unlike human soldiers, AWS could be "equipped with a wide range of different means of warfare due to their effectively unlimited physical strength. This would give them a wider selection of means to choose from in any given engagement".[258] This technological advantage could theoretically enable AWS to choose lower-impact weapons or safer attack angles, thereby enhancing compliance with precautionary obligations.[259] In the

---

and a commander have them in their arsenal and [do not] need to reserve their use for other militarily more important tasks or tasks involving higher risks for civilians, *they must use them;* Italic added.

[256] M. Homayounnejad, op. cit., p. 256.

[257] E. Winter, op. cit., p. 17.

[258] Ibid., p. 18.

[259] Ibid., pp. 17-18.

same vein — this is where emotion-based arguments are frequently invoked by proponents — it is argued that, as machines, AWS would be more precise than human combatants, lacking certain physical limitations and not being subject to psychological stress of combat,[260] they would be expandable, meaning they could "shoot second" or even sacrifice themselves in order to limit collateral damage in ways which would be impossible for human combatants.[261]

These interpretations emphasize that the obligation under Article 57(2)(a)(ii) binds commanders at the point of choosing whether or not to deploy an AWS. However, the obligation's relevance does not end here: it also extends into the operational conduct of the AWS itself once activated. In other words, while the initial choice to deploy an AWS might satisfy the commander's duty regarding the choice of means of attack, it remains necessary to assess whether the system, acting independently, can uphold precautionary obligations throughout the attack's execution.

In addition to target verification and the choice of means and methods of warfare, Article 57(2)(a)(iii) adds another obligation on the attackers to refrain from launching any attack

[260] M. Sassóli, op. cit., p. 310.
[261] Ibid., p. 336.

that may be expected to cause incidental loss of civilian life, injury to civilians, or damage to civilian objects that would be excessive in relation to the concrete and direct military advantage anticipated. This requirement builds directly on the previously discussed proportionality principle and, in practice, necessitates the ability to make complex value-based judgments that weigh military advantage against civilian harm. Here again, it is important to recall that while computational abilities might estimate harm, they cannot — for the time being — engage in the cognitive reasoning inherent in the qualitative facets of proportionality assessments.

Closely relevant, but more problematic is Article 57(2)(b), which stipulates the obligation to cancel or suspend an attack if it becomes apparent that the target is not a military objective or that the attack would cause disproportionate harm. This obligation is not only directed at those who plan or decide upon an attack, but also primarily to those who execute it.[262]

The question therefore arises whether an AWS — acting without real-time human input — can carry out the obligation to cancel or suspend an attack ? Marc Sassóli suggests that, for this obligation to be met, it is sufficient that either the system itself through technical means, or the human being using it, are

[262] M. Homayounnaejad, op. cit., p. 258.

able to acquire information indicating that the attack must be interrupted and either the machine or its human operators are able to react to such information.[263] Maziar Homayounnaejad argues that the AWS can be programmed to cancel or suspend an attack in the event that the target or target area no longer meets its programmed parameters to the correct confidence threshold.[264]

Many of the challenges associated with AWS compliance with the principle of precaution remain technical in nature. Therefore, in the absence of sufficient operational proof regarding the responsiveness and accuracy of an AWS's ability to cancel or suspend an attack in real-time — let alone reliably recognize the circumstances that would require such cancellation or suspension — it can be argued that this obligation, which rests on the capacity to reassess the proportionality and legality of an attack as the situation on the battlefield evolves, poses real difficulties. This task demands qualitative and value-based judgments that cannot simply be reduced to algorithmic thresholds or pre-programmed triggers. Consequently, the ability of AWS to independently uphold the precautionary obligations imposed by Article 57 remains

[263] M. Sassóli, op. cit., p. 320.
[264] M. Homayounnaejad, op. cit., p. 259.

doubtful, particularly in unpredictable or dynamic combat contexts, or in situations where human judgment is indispensable.

If it can be argued that the very use of an AWS could itself constitute a precautionary measure, it can equally be counterargued that human judgment — by virtue of its interpretive, contextual, and deliberative qualities — constitute a precautionary measure in its own right. One striking illustration would be the case of Stanislav Petrov.[265]

On 26 September 1983, Petrov, a Soviet officer monitoring nuclear early-warning systems, faced an alarm indicating an incoming missile strike from the United States. Protocol required him to report the alert, triggering a retaliatory strike. Yet Petrov, skeptical toward the computer-generated data, chose to override the machine's output, and to not escalate the report, preventing a catastrophic nuclear response. This example demonstrates that ultimately precaution cannot be limited to technical measures of machine-based processes, but it should encompass the contextual discernment exercised by human agents. It suggests that, while AWS might enhance certain technical aspects of precaution, they cannot substitute

[265] BBC, "Stanislav Petrov : The man who may have saved the world", BBC News, 26 Sep 2013, accessible at : https://www.bbc.com/news/world-europe-24280831

the interpretive role of human judgment — particularly where compliance with obligations such as suspension of attacks hinges on continuous, context-sensitive evaluation.

3. D. OTHER RELATED RULES OF IHL : MILITARY NECESSITY, HUMANITY, AND THE MARTENS CLAUSE

IHL is grounded in two values that serve as guiding imperatives, informing and constraining all targeting decisions, and from which the core principles derive their operational significance as they aim to strike a balance between them: military necessity and humanity.

The principle of military necessity, partially codified in Article 23(g) of The Hague Regulations of 1907 and recognized as a CIL rule, reflects the idea that the right to resort to lethal force in war is an exceptional one, which must be justified by necessity, and may only be exercised as a last resort.[266] In other words, military necessity permits only those measures indispensable to achieving a legitimate military purpose. Complementarily, the principle of humanity, enshrined in the

[266] A. Seixas-Nunes, *The Legality and Accountability of Autonomous Weapon Systems: A Humanitarian Law Perspective*, Cambridge University Press, 2022, p. 59.

St. Petersburg Declaration of 1868,[267] demands that suffering and destruction be limited to what is necessary for achieving lawful military aims, while not uselessly aggravating suffering or rendering death inevitable. The employment of any arms that would achieve such outcomes would be contrary to the laws of humanity.[268] In this sense, humanity acts as a counterweight to military necessity, ensuring that harm is not inflicted without justifiable military reason and safeguarding respect for humanitarian considerations.

Scholars address the relationship between military necessity and humanity in terms of "balance" or "compromise". For example, Homayounnaejad describes this compromise as one where military necessity permits all lawful measures intended to engage and defeat the enemy as quickly and as efficiently as possible; in contrast to humanity which forbids the infliction of any further suffering, injury or destruction that is not necessary to accomplish a legitimate military purpuse. He contends that

[267] St. Petersburg Declaration : "having by common agreement fixed the technical limits at which the necessities of war ought to yield to the requirements of humanity [...]".

[268] St. Petersburg Declaration : "That the only legitimate object which State should endeavour to accomplish during war is to weaken the military forces of the enemy; [...] This object would be exceeded by the employment of arms which uselessly aggravate the sufferings of disabled men, or render their death inevitable; That the employment of such arms would, therefore, be contrary to the laws of humanity [...]".

humanity may be seen as the logical inverse of military necessity.[269] Elliot Winter, on the other hand, clarifies that these values are not regarded as "legal principles" because they lack the normative features of legal principles, — namely, different weightings to balance against one another and the capacity to supersede positive rules.[270] Instead, IHL relies on a balance between them rather than one overriding the other, and neither possesses the ability to override explicit treaty rules without undermining the legal system.[271]

Although not clearly articulated in a single treaty, the concept of military necessity "infuses" IHL.[272] It is the fundamental rule upon which warfare relies, but it cannot justify violations of the other rules of IHL. For example, attacking surrendering or wounded troops would be unlawful because it is not essential for victory and is expressly prohibited by the Geneva Conventions.[273] Similarly, if a military commander urgently needs a transplant so save their life, harvesting organs from captives — prohibited by AP I — cannot be excused by

[269] M. Homayounnaejad, op. cit., pp. 182-183.
[270] E. Winter, op. cit., pp. 10-12.
[271] Ibid., p. 11.
[272] HRW, Losing Humanity, op. cit., p. 25; citing M. Schmitt, *Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance*, Virginia Journal of International Law, vol. 50, no. 4, 2010, p. 835.
[273] Ibidem.

the principle of military necessity, regardless of the operational need.[274] These examples show that military necessity does not absolve compliance with positive legal obligations, nor is it absolute; it is limited by humanitarian considerations, which in turn are "the *raison d'être* of humanitarian law".[275]

Thus, the relationship between military necessity and humanity frames the permissible scope of harm in armed conflict but operates within — and not above — the positive legal rules codified in IHL treaties and customary norms. Proportionality is a vivid example of the military necessity-humanity balance, as it explicitly "accepts the harsh reality of civilian harm, so long as this is 'justified' by the military advantage of attacking a lawful target; yet, it puts an upper limit on that harm."[276]

Nonetheless, Armin Krishnan warns that technological advancements can significantly influence how military necessity is assessed. He argued that once AWS are widely introduced, their use may come to be viewed as a military necessity, given their potential to outperform conventional weapons. This, in turn, could lead to a future where armed conflicts are increasingly dominated by machines — a

[274] E. Winter, op. cit., p. 11.
[275] T. McFarland, op. cit., p. 106.
[276] M. Homayounnaejad, op. cit., p. 235.

development he considers potentially disastrous.[277] Therefore, he suggests that it may be esential to restrict, or maybe even prohibit AWS from the beginning in order to "prevent a dynamic that will lead to the complete automation of war that is justified by the principle of necessity".[278]

Although the claim that AWS will be used as a matter of military necessity has been debated among scholars — and some refuted Krishnan reasoning[279] — the fact that these weapons have not yet been fully operational, and that there is no treaty that expressly addresses the conditions for their use, makes this interpretation valid as military practice could in the future shift toward their consideration as a military necessity. In that sense, their use will be limited by the principle of humanity as a counterpart to military necessity. This is where the Martens Clause becomes particularly relevant as a safeguard of humanity beyond positive law. It prevents "the assumption that anything not explicitly prohibited is permitted."[280]

The Martens Clause, codified in the preamble to the 1899 Hague Convention II and reiterated in Article 1(2) of AP I,

[277] HRW, *Losing Humanity*, op. cit., pp. 34-35; citing A. Krishman, *Killer Robots: Legality and Ethicality of Autonomous Weapons*, Routledge, 2009, pp. 91-92.
[278] Ibidem.
[279] M. Sassóli, op. cit., p. 320.
[280] N. Davison, op. cit., p. 9.

provides an additional layer of normative guidance, particularly in cases not explicitly addressed by treaty law. It affirms that in situations not covered by existing agreements,

> Civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience.

The Martens Clause thereby reinforces that humanitarian considerations continue to constrain conduct even in the absence of a specific legal prohibition. In the context of AWS, many states, civil society actors and scholars have invoked the Martens Clause to argue that delegating life-and-death decisions to machines would violate both the principles of humanity and the dictates of public conscience. Human Rights Watch, for example, contends that removing human judgment from the targeting process undermines moral accountability and the human dignity protected by IHL and international human rights law.[281]

Similarly, the ICRC emphasized the concerns raised by autonomous weapon systems under the principles of humanity and the dictates of public conscience, noting that there is *a sense*

[281] HRW, *Losing Humanity*, op. cit., pp. 36-39.

of deep discomfort with the idea of any weapon system that places the use of force beyond human control.[282]

Christof Heyns notably argued that in the human rights era, the values underlying human rights law will also influence the interpretation given to the Clause.[283] He further cautioned that the widespread public unease surrounding terms like "killer robots" reflects a deep intuitive sense that such weapons shocks this public conscience — particularly the prospect of being killed by robots — increasing the levels of anxiety among at least the civilian population.[284]

Tom McFarland adds that the *core rights-based objection to AWS* lies in the progressive removal of human involvement in the process of selecting and engaging targets. This delegation of life-and-death decisions to a weapon system effectively eliminates human judgment and human responsibility from the

---

[282] ICRC, *Statement to the Convention on Certain Conventional Weapons (CCW) Meeting of Experts on Lethal Autonomous Weapons Systems,* 13-17 April 2015, Geneva, accessible at: https://www.icrc.org/en/document/lethal-autonomous-weapons-systems-LAWS; *Italic* added.

[283] C. Heyns, *Autonomous Weapons Systems and Human Rights Law*, Presentation made at the informal expert meeting organized by the state parties to the Convention on Certain Conventional Weapons, Geneva, 13-16 May 2014, p. 4, accessible at: https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-_Informal_Meeting_of_Experts_(2014)/Heyns_LAWS_otherlegal_2014.pdf.

[284] C. Heyns, A/HRC/23/47, op. cit., p. 17 §95 and p. 18 §98.

decision to kill rendering it arbitrary, and in turn, violating the right to life.[285]

While he frames this as a "rights-based objection to AWS", the purposes of the former Special Rapporteur permit to describe it as a human-rights based interpretation of the Martens Clause. Christof Heyns' interpretation of the Martens Clause, is one of various possible interpretations. Through this lens, the Martens Clause gives more weight to humanitarian considerations, particularly to the right to life.

McFarland observes that the great challenge presented by the Martens Clause is that it has no single, generally accepted legal interpretation. The Clause "is loosely worded and invokes, without definition, concepts which are themselves susceptible of various interpretations".[286] These interpretations could range from highly restrictive to expansive. One interpretation, which according to him, has attracted significant support, is that the Clause merely confirms that customary international law continues to apply after adoption of a treaty.[287] In this sense, "the absence of a relevant treaty norm forbidding, for example, a means or method of warfare is not sufficient to establish that the means or method is permissible; it must still be assessed in

[285] T. McFarland, op. cit., p. 108 ; *Italic* added.
[286] Ibid., p. 103.
[287] Ibidem.

relation to existing rules of customary international law".[288] This represents the narrowest interpretation of the Martens Clause, according to which, the Martens Clause itself cannot serve as a basis for prohibiting a weapon; rather, a customary or conventional prohibition must be identified.[289]

Conversely, broader interpretations would either regard it as an interpretive tool or as an independent source of international law. As an interpretative tool, the Martens Clause does not define or import any substantive obligations, rather its purpose is to provide guidance in the interpretation of existing conventional and customary rules in case of doubt. This view was supported by Judge Weermantry in his dissent view in the *Nuclear Weapons Advisory Opinion*.[290] In contrast, Judge Shahbuddeen, considers that the principles of humanity and the dictates of public conscience act as independent sources of international law.[291]

---

[288] Ibidem.; Referencing Government of the United Kindgom, Written Statement in *Legality of the Threat or Use of Nuclear Weapons*, 1996, ICJ Rep 226.

[289] Ibid., pp. 103-104.

[290] Ibidem.; referencing Judge Weeramantry Dissenting Opinion in *Legality of the Threat or Use of Nuclear* Weapons, 1996, ICJ Rep 226.

[291] Ibidem.; referencing Judge Shahabuddeen Dissenting Opinion in *Legality of the Threat or Use of Nuclear* Weapons, 1996, ICJ Rep 226. Tim McFarland observes that a plain reading of Article 1(2) of AP I appears to support this view, in that it presents 'established custom', 'principles of humanity' and 'dictates of public conscience' as separate and independent

According to this view, means and methods employed in conflict must be in compliance not only with applicable conventional and customary norms but also with the principles of humanity and the dictates of public conscience.[292]

Despite the lack of consensus over a single interpretation, and regardless of the adopted interpretive approach, the fact remains that, as McFarland notes, "to date, and since its first appearance in 1899, no means of warfare has been prohibited specifically on the grounds that it would violate the Martens Clause."[293] This does not, however, make it less relevant, as the *Nuclear Weapons Advisory Opinion* stated the Martens Clause "has proved to be an effective means of addressing the rapid evolution of military technology"[294].

***

Ultimately, the legal frameworks governing AWS — whether viewed through the lens of weapons law, targeting law, or the broader principles of military, humanity, and the Martens Clause — point toward the technological capabilities of the weapon system as a key factor in determining whether AWS can

law items in a list of sources from which principles of international law may be derived. Ibid. p. 105.

[292] Ibidem.

[293] Ibidem.

[294] ICJ, Legality of the Threat or Use of Nuclear Weapons (*Nuclear Weapons Advisory Opinion),* 1996, ICJ Rep 226, §78.

actually comply IHL. While IHL provides a normative framework that prescribes obligations and limits, AWS pose a unique challenge in that, both in design and in use, they must be programmed in a way that replicates the human ability, to understand and make context-dependent, interpretive, and value-based judgments. The debate over whether AWS can perform the evaluative functions that each principle entails; the debate over military necessity and humanity; as well as the divergent interpretations of the Martens Clause, collectively highlight that — because AWS have not yet been widely operationalized — their legality cannot be assessed categorically. Instead, such an assessment must account for multiple variables: for example, the complexity of the environment of deployment, the nature of the assigned task, the technical capabilities and the sophistication of the weapon system, and the required degree of human control over the critical functions.

In order to close this legal analysis, it is now necessary to shift toward a more technical — arguably less legal — examination to AWS. The conceptual and legal understanding of AWS benefits from understanding how these systems are built and how they function. This technical inquiry will shed light on how hardware and software interact to create what is

labeled as ‘autonomy’ in the context of AWS. It will help clarify if, and why, the use of AWS could be challenging under IHL. The examination will be further supplemented by an overview of currently existing AWS, particularly, those that possess the potential to evolve into fully AWS.

CHAPTER 3–AUTONOMOUS WEAPON SYSTEMS FROM A TECHNICAL-OPERATIONAL LENS

The first Chapter illustrated more than terminological differences in definitions. Apart from the fact that these differences translate into divergent definitional approaches, they revealed that the proposals made by states, institutions, and academics are attempts to give meaning to these weapon systems or to show what they represent. This given meaning is based on an "understanding" which, particularly in the case of AWS, seems to be more subjective than objective. Each working definition reflects the perception of its author, and notably their understanding of the nature of these "weapons"; "systems"; "technologies". It reflects the "choices" they made when conceptualizing these "non-human entities".

The same applies for the second Chapter, the perception of each author is reflected in their reasoning and assumed position. If they were to perceive them as "Killer Robots"[295], then they would focus primarily on the legal, moral and ethical implications of the development and use of these systems, emphasizing the technological limitations that could lead to acts

[295] See among others: HRW, *Losing Humanity*, op. cit.; B. Docherty, *Shaking the foundations*, op. cit.; C. Heyns, A/HRC/23/47, op. cit.; R. Sparrow, *"Killer Robots"*, Journal of Applied Philosophy, vol. 24, no. 1, 2007, pp. 62-77, accessible at: http://www.jstor.org/stable/24355087.

amounting to grave violations of IHL. This viewpoint leads to the conclusion that a significant role for humans in their use must be maintained (MHC), since legal responsibility cannot be attributed to machines.

If they were to perceive them as "means of warfare"[296] used by combatants, they would need to approach them from a technical and operational viewpoint to assess their legality. What are they? How do they function? Would this method of functioning be *per se* problematic from an IHL perspective? This approach would also potentially lead to MHC in order to establish intent, agency and avoid responsibility gaps. In this sense, there is currently a consensus, regardless of the adopted approach, on the need for human control to ensure compliance with international humanitarian law, international criminal law and responsibility regimes.[297] The divergence remains, however, over the characteristics and scope of this control.

In a similar vein, the United Nations Institute for Disarmament Research (UNIDIR) observed that

---

[296] See among others: A. B. Fisher, op. cit.; M. Sassóli, op. cit.; V. Boulanin and M. Verbruggen, op. cit.; E. Winter, op. cit.

[297] See Stop Killer Robots, *Growing Consensus on Policy at UN Discussions on AWS but Skepticism Towards Non-Binding Principles & Practices*, 2022, accessible at: https://www.stopkillerrobots.org/news/growing-consensus-on-policy-at-un-discussions/ ; A. Guterres, A/79/88, op. cit., p. 6 §12.

> proponents and opponents of AWS will seek to establish a definition that serves either their aims and interests. The definitional discussion will not be value neutral discussion of facts, but ultimately one driven by political and strategic motivations.[298]

Similarly, Paul Scharre observes that :

> Countries view autonomous weapons through the lens of their own security interests. Nations have very different positions depending on whether or not they think autonomous weapons might benefit them.[299]

Drawing on these observations; if we shift to a macro perspective, fully AWS would be nothing more than one facet of the broader international technology race — fueled by the belief that the nation that exploits AI first will become the ruler of the world.[300] Logically, it follows that achieving such a strategic advantage would be even more advantageous if it were in the military sphere. As such, some opinions will either support — or at least not oppose — the development of the

---

[298] UNIDIR, *The Weaponization of Increasingly Autonomous Technologies,* op. cit., p. 22.

[299] P. Scharre, *Army of none*, op. cit., p. 345.

[300] R. Gigova, "*Who Vladimir Putin thinks will rule the world*," CNN, 2017, accessible at: https://edition.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html; quoting V. Putin: "Artificial intelligence is the future not only of Russia but of all of mankind [...] Whoever becomes the leader in this sphere will become the ruler of the world [...]" ; see also, G. Chen, Opinion | *In AI race against US, China is racking up real-world wins*, 2025, accessible at: https://www.scmp.com/opinion/china-opinion/article/3307357/ai-race-against-us-china-racking-real-world-wins.

technologies enabling autonomy in weapon systems; this line of thinking can point to their potential conformity with international humanitarian law by emphasizing the benefits they would represent[301] — without necessarily endorsing their use.[302]

Conversely, others will reject their use in principle, but nonetheless acknowledge the necessity of researching them for national security purposes. For example, both France and the United Kindgom emphasize the importance of maintaining human control over AWS and publicly deny any intent to deploy fully autonomous weapons. Yet, their national documents frame the development of such technologies as a national security matter, should others actors decide to use them against them.[303]

---

[301] See among others: A. Etzioni and O. Etzioni, op.cit., p.72-74; M. Schmitt, op. cit.; M. Sassóli, *op. cit*.; E. Winter, op. cit.

[302] A parallel can be–cautiously–drawn with nuclear weapons, which continue to be developed, acquired, and modernized as part of the doctrine of Mutual Assured Destruction often framed as a form of insurance or for deterrence purposes. Similarly, AWS are argued to be developed not necessarily for operational use, but for their strategic or technological advantages. See H.D. Sokolski (ed.), *Getting MAD: Nuclear Mutual Assured Destruction, Its Origins and Practice*, Strategic Studies Institute, 2004, accessible at: https://apps.dtic.mil/sti/tr/pdf/ADA428336.pdf.

[303] See Ministère des Armées (France), *Opinion on the Integration of Autonomy into Lethal Weapon Systems*, Defense Ethics Committee, 2021, pp. 20-23 accessible at: https://cd-geneve.delegfrance.org/IMG/pdf/defence_ethics_committee_-_opinion_on_the_integration_of_autonomy_into_lethal_weapon_systems.pdf ; Ministry of Defence (United Kingdom), *The Government Response to the Report by the House of Lords AI in Weapon Systems Committee: 'Proceed with Caution: Artificial Intelligence in Weapon Systems'*, Session

This observation is corroborated by the fact that specialized studies and reports indicate that, except for loitering munitions — widely recognized as the only existing category of offensive autonomous weapons currently in operation,[304] the majority of autonomous systems developed or under development are primarily defensive systems.[305]

However, if we add an additional observation — namely, the increasing and extensive use of loitering munitions in contemporary armed conflicts; their integration with AI-enabled targeting systems; and the progressive reduction of human control in the targeting cycle[306] — we are compelled to ask whether these systems, when viewed as a whole, are not in fact collectively constituting an "autonomous weapon system".

As such, the pressing question becomes whether the legal and ethical objection is narrowly focused on the development of a single, "all-in-one" device formally labeled as an autonomous weapon system. If so, this threshold can — and has — already been bypassed by military actors and manufacturers through the

2023-24 HL paper 16, 2024, p. 5 §11, accessible at: https://assets.publishing.service.gov.uk/media/65cb77caa7ded0000c79e526/Government_response_to_the_House_of_Lords_AI_in_Weapon_Systems_Committee_Report.pdf.

[304] V. Boulanin and M.Verbruggen, op. cit., p. vii.

[305] Ibidem.

[306] See Section 2 of this Chapter : AWS in recent armed conflicts.

integration of different semi-autonomous, supervised-autonomous modes, and AI-enabled components. However, if the real objection lies in the broader shift toward a warfare that is rendered increasingly autonomous, thereby challeging the longstanding human-centric paradigm as a foundation to the law of armed conflict, then the discussion must evolve. It should move beyond narrow technical classifications and focus instead on the actual conduct of warfare — specifically, on whether human control over targeting decisions remains meaningful, informed, and effective, rather than symbolic or automated by default.

Consequently, to grasp the operational implications of AWS, it is necessary to first understand how these systems are built and how they function. Section 1 of this Chapter lays the technical foundations by examining the architecture and foundational technologies of AWS and the role of AI in shaping their behavior and capabilities. This exploration sets the stage for Section 2, which moves from theory to practice by exploring existing AWS and their documented use in real-world armed conflicts. Through these illustrative examples, the section aims to shed light on how these technologies have already been deployed, the level of autonomy involved, and the legal and humanitarian challenges that arise when theory meets battlefield

reality. Though, throughout this analysis, the use of terms such as "autonomy", "cognition", "intelligence", etc. to describe AWS — even if contested[307] — is deemed useful in highlighting the controversies surrounding the nature and implications of such systems.

SECTION 1– ARCHITECTURE AND TECHNICAL FOUNDATIONS OF AUTONOMOUS WEAPON SYSTEMS

> 1. A robot may not injure a human being or, through inaction, allow a human being to come to harm.
> 2. A robot must obey orders given to it by human beings except where such orders would conflict with the First Law.
> 3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.[308] — Three Laws of Robotics, Isaac Asimov, 1942.

The *Three Laws of Robotics*, developed by science-fiction writer Isaac Asimov in the 1940s, were meant to create an ethical system governing the relationship between humans and robots. Although fictional, Asimov's laws later became

[307] R. Surber, *Artificial Intelligence: Autonomous Technology (AT), Lethal Autonomous Weapons Systems (LAWS) and Peace Time Threats*, ICT for Peace Foundation and the Zurich Hub for Ethics and Technology (ZHET), 2018, p. 1 and p. 20.
[308] I. Asimov, "*Runaround*", I, Robot, 1942.

highly influential in discussions about technology, particularly, robotics and artificial intelligence.[309] The three laws were later supplemented by another law, known as the 'zeroth law', that superseded the others. It stated that "a robot may not harm humanity, or by inaction, allow humanity to come to harm." [310]

Today, Asimov's vision is significantly challenged by the rise of AWS. The *Killer Robots* or *Lethal Autonomous Robotics*, are designed to select (i.e., search for, detect, identify, track, or select) and engage (i.e., use force against, neutralize, damage, or destroy) targets, with no human intervention after activation. As weapons, they are designed for a purpose: a mean to kill, cause injury, damage, and/or destroy. Despite the dystopian mental image one might draw, some argue that — as demonstrated in the previous Chapter — on the contrary, AWS can be a guarantee for better compliance with IHL, refuting the

[309] See A. Guterres, A/79/88, op. cit., pp. 137-138, Civil Affairs Institute submission; see also S. L. Anderson, *Asimov's "Three Laws of Robotics" and Machine Metaethics, AI & Soc*, Springer Nature Link, Vol. 22, 2008, accessible at: https://link.springer.com/article/10.1007/s00146-007-0094-5; S. Benson, *Prosecuting Asimov's Nightmare: Killer Robots and the Law of War*, Georgetown Security Studies Review, 2024, accessible at: https://georgetownsecuritystudiesreview.org/2024/03/04/prosecuting-asimovs-nightmare-killer-robots-and-the-law-of-war/.

[310] The Editors of Encyclopaedia Britannica, "Three laws of robotics", Encyclopedia Britannica, 2025, accessible at : https://www.britannica.com/topic/Three-Laws-of-Robotics.

idea of banning them.[311] AWS are reportedly faster and better than humans in processing large amounts of data.[312] Immune to human negative feelings such as vengeance, hate, stress, fatigue, or psychological traumas, they can be better compliant with the principles of IHL.[313]

In this sense, the case *for* AWS can be just as valid as the case *against* them. The determining factor becomes technological feasibility.

The technology-centric definitions imply that these systems are futuristic — something that has yet to be developed —, that they would have to have 'cognitive' abilities akin to those of humans to be considered truly autonomous.[314]

Cognition can be defined as

> The mental action or process of acquiring knowledge and understanding through thought, experience, and the senses. It encompasses various aspects of high-level intellectual functions and processes such as attention, memory, knowledge, decision-making, planning, reasoning,

[311] See among others: M. Schmitt; E. Winter; M. Sassóli op. cit.
[312] E. Winter, op. cit., p. 7; citing M. Ekelholf, *Lifting the Fog of Targeting: 'Autonomous Weapons' and Human Control through the Lens of Military Targeting*, Naval War College Review 61, vol. 71(3), 2018, p. 79 and p. 83, accessible at: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=5125&context=nwc-review.
[313] M. Schmitt, op. cit., p. 13; E. Winter, pp. 4-5 and p. 7.
[314] Ministry of Defence (United Kingdom), *Joint Concept Note 1/18*, op. cit., p. 60.

> judgment, perception comprehension, language, and visuospatial function.[315]

In humans, cognition encompasses perception, reasoning, decision-making and judgment. Functions that the majority of which can be — to a certain extent — mimicked or replicated in machines. However, substantially, cognition — particularly decision-making and judgment — is not about mere raw information or data processing, but rather the ability to *contextualize* this information, by interpreting meaning, exercising judgment, reflecting on consequences and drawing conclusions that are not only cognitive in nature, but also morally saturated and based on past learnt experiences.

Cognition, in the context of machines, can be understood as to the machine's programmed or learned capacity to perceive (sense), interpret and evaluate (think/decide), and respond to complex inputs in a battlefield environment (act).[316] It allows

[315] A. Dhakal and B.D. Borbin, *Cognitive Deficits*, StatPerls Publishing, PMID: 32644478, Excerpt, 2025 accessible at : https://pubmed.ncbi.nlm.nih.gov/32644478/.

[316] ICRC, *Autonomy, artificial intelligence and robotics: Technical aspects of human control*, op. cit., p. 7: " An autonomous (robotic) system or function is closed loop ("sense-think-act"). The machine receives information from its environment through sensors ("sense"); processes these data with control software ("think"); based on its analysis, performs an action ("act") without further human intervention"; V. Boulanin and M. Verburggen, op. cit., p. 7 "autonomy (in a physical system) is always enabled by the integration of the same three fundamental capabilities: sense, decide and act".

the system to assess threats, prioritize actions, and adapt to complex and evolving battlefield conditions, often through the use of advanced computational models.

A simple way to understand how the machine *senses*, *thinks*, and *acts*, and where AI fits in this scheme, is to draw an analogy with a human being. Just like a human, an AWS is essentially composed of two components : a body (hardware) (A) and a brain/mind (software) (B).

A. THE HARDWARE

The hardware of an AWS refers to the tangible components that allow the system to interact with the physical environment. This includes *sensors* (eyes and ears) which allow the system to collect raw data from its environment; *actuators* (muscles) and *effectors* (hands and legs) which allow the system to move, position and apply force. All of these elements are integrated into a *platform*, which could be a drone, a ship, or a ground robot, among other types.

In other words, an AWS would be physically composed of mechanical components (engines, wheels, wings, etc.), a sensor suite (cameras, microphones, radar, infrared, etc.) and the weapon payload (missiles, explosives, guns, etc.) that together allow it to move, observe, and deliver force.

1. SENSORS

A sensor can be defined as "a device that responds to physical stimulus (such as heat, light, sound, pressure, magnetism, or a particular motion) and transmits a resulting impulse".[317] It can take many forms: radar sensor, thermic sensor, infrared sensor, GPS, visual cameras, among others.[318]

Sensors are fundamental for enabling autonomy in weapon systems since they allow the system to "sense" and gather data from the world.[319] Since no single type of sensor can provide complete situational awareness and a coherent understanding of the environment, an AWS may be equipped with various sensors working simultaneously.[320] This process is referred to as *sensor fusion* — where responses from multiple independent sensors of different types are combined to provide reinforced responses.[321]

---

[317] Merriam-Webster Dictionary, "Sensor" : https://www.merriam-webster.com/dictionary/sensor ; J. Fraden, *Handbook of Modern Sensors: Physics, Designs, and Applications*, 3rd ed., Springer, United States, 2004, p. 1, defines a sensor as a device that receives and responds to a signal or a stimulus.

[318] ICRC, *Autonomous Weapon Systems Implications of Increasing Autonomy in the Critical Functions of Weapons*, op. cit., p. 36.

[319] ICRC, *Autonomy, artificial intelligence and robotics*, op. cit., p. 7; V. Boulanin and M. Verburggen, op. cit., p. 8.

[320] For example video cameras for visual recognition, infrared sensors for heat signatures, radar, or LIDAR for detecting range and movement, acoustic sensors for sound, etc.

[321] J. Fraden, op. cit., p. 524.

By fusing inputs from different sensors, an AWS's control system can "see" or "perceive" the battlefield in a more robust way.[322] In this sense, the weapon's effectiveness is fundamentally constrained by the physical capabilities, reliability, and precision of its sensors. However, from an IHL perspective, the reliance of AWS on sensors introduces challenges for compliance — particularly with the principle of distinction. Sensors operate by detecting physical properties (heat, movement, electromagnetic signals, etc.) but they do not assess legal status. While they can enhance a system's ability to detect objects or persons, they remain limited to recognizing patterns, meaning they cannot exercise legal or moral judgment in distinguishing lawful from unlawful targets under IHL. For example, a thermal sensor may detect and identify a heat-emitting figure but cannot, independently, determine whether the figure is a combatant, a civilian, or a *hors de combat*.[323]

[322] For example, it might use camera, infrared and LIDAR data together to determine whether a human-shaped figure is alive (warm or moving body). This sensor fusion is critical for enabling software functions such as Automated Target Recognition (ATR) and computer vision, both of which rely on sensor data to classify, identify, and track targets. See ICRC, *Autonomy, artificial intelligence and robotics: Technical aspects of human control*, op. cit., pp. 19-20.

[323] ICRC, *Autonomous Weapon Systems Implications of Increasing Autonomy in the Critical Functions of Weapons,* op. cit*.,* p. 79.

2. ACTUATORS

Once the data has been gathered and processed, the actuators then receive signals from the system's control software to carry out the necessary movement. An actuator is "a mechanical device [used] for moving or controlling something."[324] It is the part of a machine that is responsible for moving and controling components by converting energy into physical motion.[325] To analogize, they are the equivalent of "muscles" in human beings: they generate the motion which will move the end-effectors.[326] They can take the form of electric motors, batteries or cylinders, depending on the nature and energy requirements of the system.

In this sense, actuators are not directly responsible for applying force themselves; rather, they convert the system's decision into physical behavior by putting end-effectors in motion: firing a weapon, deploying munitions, or maneuvering into position, etc. Their function is to execute outputs generated by the system's control algorithms, thereby bridging the sensing and the acting phases.

---

[324] Merriam-Webster Dictionary, "Actuator" : https://www.merriam-webster.com/dictionary/actuator

[325] LINAK, *What is an actuator?* 2024, accessible at : https://www.linak.com/products/linear-actuators/what-is-an-actuator/

[326] Ibidem.

From an IHL perspective, actuators can be problematic in cases of mechanical failure. For example, if an actuator fails, jams, or misfires it could directly affect the distinction and proportionality outcomes of the attack.[327] Therefore, their mechanical limitations must be accounted for in legal reviews, as mandated under Article 36 of PA I, since their performance impacts whether the AWS can operate in compliance with IHL in all expected circumstances of use.

3. END-EFFECTORS

End-effectors refer to "any of various tools that can be mounted at the end of a robotic arm and that are used to interact with or manipulate objects".[328] Simply put, end-effectors are the primary means by which robots interact with their environment.[329] In the context of AWS, they represent the final link in the action chain of a weapon system, serving as the

[327] To illustrate, if an actuator controlling a drone's targeting mechanism cannot adjust trajectory after detecting new civilian presence, the AWS risks executing an unlawful attack.

[328] Merriam-Webster Dictionary, "End-Effector" : https://www.merriam-webster.com/dictionary/end%20effector

[329] N.A. Lad, Y.P. Ballal, and P.D Kulkarni, *Study of End Effectors–A Review*, International Journal of Trend in Research and Development, Vol. 2 nº. 5, 2015, p. 365, accessible at: https://www.ijtrd.com/papers/IJTRD201.pdf ; R. Rao, *What are End Effectors? Types of End Effectors in Robotics and Applications*, Wevolver, 2024, accessible at: https://www.wevolver.com/article/end-effector.

physical mean through which the system exerts force.[330] In this sense, the effectiveness of an AWS depends not only on accurate perception and internal processing, but also on the precision, speed, and adaptability of its end-effectors. This is particularly relevant in complex combat scenarios, where the target may not be stationary or even known in advance. Therefore, choosing the right end-effector can be a complex and vital decision as it can highly impact the robot's precision and efficiency.[331]

From an IHL perspective, end-effectors in AWS raise challenges of compliance with the principles of distinction and proportionality. As the physical means by which force is applied, they translate targeting decisions into real-world effects. Their design and capabilities directly influence whether an AWS can limit its effects to lawful military targets and avoid excessive collateral harm.[332] Moreover, end-effectors can make

[330] They typically correspond to the weapon delivery mechanisms (e.g., missile launchers or kinetic projectiles) that translate the system's outputs into tangible force, though not limited to lethality.

[331] This choice would primarily depend on the task requirements, the end-effector capabilities, its compatibility with the robotic system, as well as the expected cost; See R. Rao, *What are End Effectors? Types of End Effectors in Robotics and Applications*, op. cit.

[332] For example, the use of high-explosive projectiles weapons as end-effectors increases the risk of indiscriminate and uncontrollable effects in populated environments. See next section: AWS in recent armed conflicts. Particularly the case studies on Ukraine and Gaza.

the AWS unlawful *per se*, if it used a weapon banned under IHL as a payload. Therefore, the nature, reliability, and adaptability of end-effectors cannot be merely considered as technical issues — they are central to determining whether an AWS can be lawfully developed and used under the rules of IHL.

The hardware elements (sensors, actuators, and end-effectors) work in a tightly coordinated loop: sensors gather input from the environment, actuators generate movement based on commands, and the end-effectors execute the final task. They are inherent to both the Sense and Act stages of a system, and are not — as briefly illustrated — legally neutral: each of the physical components raises challenges for compliance with IHL. In this sense, the design and performance of hardware components can either facilitate or contravene the system's ability to adhere to IHL principles. As such, any review of AWS legality must account not only for the algorithms that guide the system, but also for the physical architecture that enacts its decisions.

Yet, even with sophisticated hardware, autonomy remains incomplete without the *software* (brain) that governs how the system processes information and makes decision. This software is the key component of AWS as it is the element that

allows — or will allow — the system to complete the targeting cycle on its own, without human intervention.

B. THE SOFTWARE

In a broad sense, software are computer programs or instructions that control what a computer can do.[333] In the context of AWS, the software is the component that allows the system to "think", meaning that it interprets the data it receives from sensors, determines the appropriate course of action, and activates the relevant physical components to carry out that decision. In this sense, the software is the core enabler of autonomy, governing every stage of the system's operation.[334]

---

[333] Cambridge Dictionary, "Software" (Cambridge University Press): https://dictionary.cambridge.org/dictionary/english/software; A software can also be defined as "the entire set of programs, procedures, and related documentation associated with a mechanical or electronic system and especially a computer system", see Merriam-Webster Dictionary, "Software": https://www.merriam-webster.com/dictionary/software ; or as a program or set of programs designed to perform specific tasks on a computer , see Taclia, *What is Software? Definition, types and examples of use*, 2025, accessible at: https://www.taclia.com/en-us/blog/what-is-software ; L. Manovich defines it as combination of data structure and set of algorithms, see L. Manovich, *Software Takes Command, International Texts in Critical Media Aesthetics*, Vol. 5, Bloomsbury Academic, 2013, p. 207, Accessible at: https://library.oapen.org/bitstream/handle/20.500.12657/58738/9781623566722.pdf?sequence=1&isAllowed=y.

[334] V. Boulanin and M. Verbruggen, op. cit., p. 12. As Vincent Boulanin and Maaike Verbruggen observe the technologies that are deemed the most critical to autonomy are the software elements. They note that it is the complexity of the sensing, modeling, and decision-making software that actually determines the level of autonomy of a system.

Particularly, the targeting process is governed by a key software component known as the *control system*, which translates mission goals and environmental feedback into specific commands issued to the hardware, thereby guiding the system's actions.[335] This control system is said to "[step] into the shoes" [336] of the human operator to some extent, as it assumes roles traditionally carried out by human judgment and decision-making.[337] Thus, to fully grasp how software governs autonomous decision-making in combat scenarios, it is essential to move beyond the internal processing structures and examine how AWS interact with dynamic operational environments and by which means.

[335] V. Boulanin and M. Verburggen, op. cit., p. 9.
[336] T. McFarland, op. cit., p. 33.
[337] As Tom McFarland notes, the discipline that deals with regulating the behaviour of a machine over time is known as the control theory. He explains that designers of automated or autonomous system generally model the systems they design as consisting of two main components: the controlled machine or process (e.g., a drone or a loitering munition) and the controller (the control system which governs the behaviour of that machine). If the machine is not capable of autonomous operation, it would be directly operated by a human (non-autonomous systems), conversely, when a manual system or process is replaced with a system capable of some degree of autonomous operation (semi-autonomous or supervised autonomous), this is when the control system "steps into the shoes" of the human operator to some extent. Ibid., pp. 31-32.

1. THE SOFTWARE AND THE OODA LOOP

Discussions about autonomy in weapon systems are often framed in terms of the OODA loop — Observe, Orient, Decide, and Act. This loop is similar to the weapon's internal loop previously discussed (Sense-Think-Act) but it is external and broader. With a manual system, all steps of the loop are completed by a human: observing the environment to extract raw information; orienting oneself in relation to the environment by processing that information; making a decision based on that model; and acting on the decision.[338] In this sense, the purpose of developing AWS would be to assign part or all of the loop to the machine in order to realize some operational advantage such as greater speed or endurance.[339]

On AWS and the OODA loop, Shin-shin Hua, a Research Affiliate at the Centre for the Study of Existential Risk at the University of Cambridge, explains — drawing on other scholars' analyses — that in warfare, the Observe stage of the targeting process has long been carried out by machines and that this use is generally uncontroversial from an IHL perspective.[340] Similarly for the Act stage, once the military target and how

[338] Ibid. p. 35.
[339] Ibidem.
[340] S. Hua, op. cit., pp. 122-123.

lethal force is delivered (e.g., choice of weapon, operational parameter and timing) have been determined by a human operator, the delivery of lethal force itself has already been widely automated through use of remote warfare.[341] Nevertheless, controversies arose when the development of machine learning (ML) technologies opened up the possibility that AWS might also be used to carry out the Orient and Decide stages of the targeting process typically carried out by an experienced human commander.[342]

In such a case, during the Orient phase, an AWS would autonomously review current intelligence estimates, sensor collection, and battlefield reports. It would evaluate the tactical strategic implications of this information, along with other military and non-military considerations, to identify potential courses of action.[343] The weapon would then use ML to determine the best course of action to be executed at the subsequent Decide stage — which represents the final deliberative step in the decision-making cycle and ultimately results in the application of force during the Act stage.[344]

[341] Ibidem.
[342] Ibidem.
[343] A. L. Schuller, op.cit., p. 394.
[344] S. Hua, op. cit., p. 123.

In other words, before AWS, existing systems were already 'autonomously' deployed uncontroversially in two stages of the OODA loop. First, the Observe stage where the goal is to form initial situational awareness through reconnaissance and surveillance, i.e., to gather intelligence and for targeting support or to identify potential threats or targets, then relay information to human operators/commanders. Human commanders would in turn exercise the most critical step: Orient, which involves interpreting what has been observed and contextualizing it. Ultimately, this step shapes how the next stage Decide is made: the human would select a course of action, after *consciously* weighing it against various other options and considerations leading to the Act stage, which in this context, is effectively applying force to the target.

2. DELEGATING DECISION-MAKING TO SOFTWARE

It was previously mentioned that, depending on the adopted approach, AWS could encompass existing weapon systems that feature some degree of autonomy in certain functions, just as much as they could be restricted to systems capable of performing "cognitive" tasks that mirror human intelligence (situational awareness or evolving learning capabilities). In fact, developing weapons that would exhibit

such advanced cognitive capabilities is theoretically possible, but only when *General Artificial Intelligence* (GAI) has been developed — which is not currently the case.[345] At present, all existing weapon systems that are AI-enabled rely on *Narrow* AI.

Although AI is not a prerequisite for autonomy in weapon systems, it is undisputed that it greatly enhances it when integrated into the system.[346] Unlike General AI, which aims to replicate human intelligence, or *Superintelligent* AI, which seeks to surpass it, Narrow AI is designed to carry out specific tasks within known limitations of technology and computing power.[347] Thus, despite real advances in AI across many fields, today's AI remains "narrow" or "weak" — it operates through pre-programmed instructions and turns tasks into algorithms and calculations that a software can perform.[348]

---

[345] Syracuse University School of Information Studies, *Types of AI: Explore Key Categories and Uses*, 2025, accessible at: https://ischool.syracuse.edu/types-of-ai/; see also: IBM, *Understanding the different types of artificial intelligence*, 2023, accessible at: https://www.ibm.com/think/topics/artificial-intelligence-types; M. Damar, A. Özen, U.E. Çakmak, E. Özoğuz, F.S. Erenay, *Super AI, Generative ai, Narrow AI and Chatbots: An Assessment of Artificial Intelligence Technologies for the Public Sector and Public Administration*, Journal of AI. Vol. 8(1), 2024, pp. 85-88.

[346] ICRC, *Artificial intelligence and machine learning in armed conflict: A human-centered approach*, International Review of the Red Cross, Digital technologies and war, vol 102, nº. 913, 2020, p. 466.

[347] Syracuse University School of Information Studies, op. cit.

[348] Ibidem.

From a technical standpoint, delegating decision-making to machines — especially in the context of targeting decisions — relies essentially on programming.[349] Broadly speaking, no matter how complex the task is, as long as it can be programmed, it can — in principle — be performed by the machine. In this sense, autonomy in a weapon system will depend on "the ingenuity of human programmers and developers to find a way to break down a problem into mathematical rules and instructions that the computer will be able to handle."[350]

Specifically, the way by which the Orient and Decide stages can be delegated to a system can follow two principal paths, each reflecting different levels of autonomy and a different set of technical and legal implications. The first is rule-based decision-making, where the system follows pre-programmed logic set by human developers, i.e., fixed algorithms with explicit if-then rules. In such cases, even though the system appears to make decisions, it is essentially executing instructions previously determined by a human, without any

[349] Computer scientists conceptualized the intellectual work of programming as consisting of two interconnected parts: creating the data structures which logically fit with the task which needs to be done and are computationally efficient, and defining the algorithms which operate on these data structures. See L. Manovich, op. cit., pp. 207-208.
[350] V. Boulanin and M. Verburggen, op. cit., p. 12.

capacity to adapt or learn beyond these parameters.[351] This method is generally easily traceable and predictable, but it can be limited in flexibility when facing unforeseen scenarios.[352] The second, more controversial path, is machine learning-based decision-making, where the system is capable of generating output and adapting its responses based on training data or real-time environmental feedback. As the name suggests, this allows the software to "learn" and improve its performance over time.[353]

i. MACHINE LEARNING SYSTEMS

> A machine learns whenever it changes its structure, program, or data (based on its inputs or in response to external information) in such a manner that its expected future performance improves.– Niles J. Nilson, 1998.[354]

Before ML, humans were the only ones programming systems — they would define the inputs, outputs, and processes. Because all these parameters were fixed, the system was

---

[351] H. Roff, *Distinguishing autonomous from automatic weapons*, op. cit.; S. Hua, op. cit., pp. 123-124; V. Boulanin and M. Verburggen, op. cit., p. 9.

[352] V. Boulanin and M. Verburggen, op. cit., p. 9 and p. 16.

[353] S. Hua, op. cit., p. 124.

[354] N. J. Nilson, *Introduction to Machine Learning: An Early Draft of a Proposed Textbook*, Robotics Laboratory, Department of Computer Science, Standford University, 1998, p. 1, accessible at: https://ai.stanford.edu/~nilsson/MLBOOK.pdf ; cited by V. Boulaning and M. Verburggen, op. cit., Box 2.2., p. 16 .

considered *deterministic*, based on simple "if/then" rules (e.g., if a certain weight is detected, then detonate). ML alters this dynamic by involving the software in its own development. The human may still provide the input data, but the system learns through training and can draw conclusions or make predictions without explicit human instructions at every step.[355]

The complexity further intensifies when *Reinforcement Learning* (RL) and *Deep Learning* (DL) become part of the equation, as both significantly shift how machines learn from and interact with their environment. RL is inspired by behavioral psychology (trail and error, reward and punishment).[356] In the context of AWS, it is used to enhance decision-making, such as determining the best path or tactic to achieve a goal, adapting in real-time to new battlefield

[355] S. Brown, *Machine learning, explained*, MIT Management Sloan School of Management, 2021, accessible at: https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained.

[356] ICRC, *Autonomy, artificial intelligence and robotics: Technical aspects of human control*, op. cit., p. 16. See also V. Boulanin and M. Verburggen, op. cit., Box 2.2., p. 16. RL refers to the process by which the machine receives some reward for its action and obtains more rewards when the outcome is closer to the desired outcome, however, that desired outcome is never presented to the machine.

information, or choosing between multiple targets based on learned priorities.[357]

Conversely, DL is primarily modeled after the human brain (neural networks).[358] In the context of AWS, it is mostly used for perception (e.g., object recognition, target identification based on images or sensor data, tracking dynamic or moving targets).[359] To simply illustrate: to recognize a face,

---

[357] See among others: Z. Hong-Peng, *Maneuver Decision-Making Through Automatic Curriculum Reinforcement Learning Without Handcrafted Reward functions*, arXiv, 2023, accessible at: https://arxiv.org/pdf/2307.06152 ; H. Lee, S. Park, W.J. Yun, S. Jung and J. Kim, *Situation-aware deep reinforcement learning for autonomous nonlinear mobility control in cyber-physical loitering munition systems*, arXiv, 2022, accessible at: https://arxiv.org/pdf/2301.00124; S. Li, X. He, X. Xu, T. Zhao, C. Song and J. Li, *Weapon-target assignment strategy in joint combat decision-making based on multi-head deep reinforcement learning*, IEEE Access, 2023, accessible at: https://www.researchgate.net/publication/374693028_Weapon-Target_Assignment_Strategy_in_Joint_Combat_Decision-Making_based_on_Multi-head_Deep_Reinforcement_Learning.

[358] DL refers to a method where a system tries to 'think' like a brain by using artificial neural networks with many layers. It enables the system to identify and interpret complex patterns within data. See J. Holdsworth, *What is deep learning?* IBM, 2024, accessible at: https://www.ibm.com/think/topics/deep-learning.

[359] See among others: A.K. Dogra, V. Sharma, and H. Sohal, *A survey of deep learning techniques for detecting and recognizing objects in complex environments*, Computer Science Review, vol 54, 2024, accessible at: https://www.sciencedirect.com/science/article/abs/pii/S1574013724000704; H. Sun, *Image Target Detection and Recognition Method Using Deep Learning, Advances in Multimedia*, vol. 2022, Issue 1, 2002, accessible at: https://onlinelibrary.wiley.com/doi/10.1155/2022/4751196; V. Boulanin and M. Verburggen, op. cit., p. 17.

DL identifies several layers, it first detects lines; then shapes; then identifies a nose, a mouth, eyes — the combination of these layers enable it to recognize this structure as a face.

Although these techniques significantly increase the efficiency of computational systems, their use in AWS can introduce major challenges from an IHL perspective — particularly in terms of predictability.[360] Two of their most pressing challenges are the "black box problem" and the challenges stemming from the system's mode of learning.

ii. LIMITATIONS AND CHALLENGES OF MACHINE LEARNING

The black box problem arises when the internal decision-making process of the system becomes opaque, even to its developers. [361] Unlike traditional systems governed by deterministic, rule-based logic, ML systems derive their rules from data, which often results in complex algorithmic structures that even developers cannot fully interpret. In other words, with ML techniques, humans may understand the input data and

[360] V. Boulanin and M. Verburggen, op. cit., p. 11 and p. 17; ICRC, *Artificial intelligence and machine in armed conflict: A human-centred approach*, op. cit., pp. 475-476; S. Hua, op. cit., pp. 127-128.
[361] ICRC, *Artificial intelligence and machine in armed conflict: A human-centred approach,* p. 476; ICRC, *Autonomy, artificial intelligence and robotics: Technical aspects of human control*, op. cit., p. 3 and pp. 15-16; V. Boulanin and M. Verburrgen, op. cit., p. 25.

observe the resulting output, but they are often unable to determine the precise reasoning process or steps the system followed to reach its conclusion.[362]

This lack of explainability not only undermines trust in the system but also complicates the attribution of legal responsibility and the assessment of compliance with principles such as distinction and proportionality.[363] The fact that an AWS selects and engages targets without its operators or developers being able to explain how those decisions were reached, makes verifying compliance with targeting principles, in all circumstances, nearly impossible. Moreover, the use of learning algorithms increases the unpredictability of AWS behaviour, since the system may adapt over time or respond differently to similar inputs in future scenarios. This lack of unpredictability can pose particular concerns where the failure to predict the system's action could result in unlawful harm to civilians or *hors de combat* persons.[364]

In addition to the black box nature, the different modes of learning that may be used by the system can themselves be

[362] V. Boulanin and M. Verburggen, op. cit., p. 17.
[363] Stop Killer Robots, *Facts about Autonomous Weapons*, n.d., accessible at: https://www.stopkillerrobots.org/stop-killer-robots/facts-about-autonomous-weapons/.
[364] ICRC, *Autonomy, artificial intelligence and robotics: Technical aspects of human control*, op. cit., p. 10; M. Homayounnejad, op. cit., p. 69.

problematic. It should be noted that there are two forms of training: *offline training* (before deployment) and *online learning* (ongoing learning after deployment).[365] In offline learning, the system is trained on a fixed dataset during development and its training stops before use.[366] By contrast, in online learning, the system continues to learn and adapt from new data after its deployment. This means that an AWS can change its behavior over time in response to changing environments and constant interactions in a live battlefield.[367]

AWS may be trained using *supervised* or *unsupervised* learning, to identify and generalize patterns from data. In supervised learning, the machine is trained using datasets that are pre-labeled with correct answers.[368] For example, systems can learn image recognition by scanning databases with tagged images, (it may learn to distinguish between a tank and a school bus by processing thousands of tagged images). Unsupervised learning, by contrast, involves training the system on raw, unlabeled data, where it must find patterns in the data itself with

[365] ICRC, *Autonomy, artificial intelligence and robotics: Technical aspects of human control*, op. cit., p. 15.
[366] Ibidem.
[367] M. Homayounnejad, op. cit., p. 61; V. Boulanin and M. Verburggen, op. cit., pp. 25-26.
[368] M. Homayounnejad, op. cit., p. 59.

no known answers fed into the system.[369] This method is particularly challenging under IHL because the system may draw conclusions or make targeting decisions based on self-generated patterns that are unpredictable to the human operator.[370] Additionally, it may lead to wrongful classification of objects, misidentification of threats or disproportionate use of force.

Moreover, machine learning systems are said to be "data intensive"[371] — meaning that in order to learn, the system must be supplied with large volumes of training data. They would learn by abstracting statistical relationships from these inputs.[372] However, the datasets used in training the system can raise their own challenges — notably, *bias*.

In simple terms, bias means the system may make incorrect or flawed decisions because of how it was trained or how it processes information. This presents a critical concern in the context of AWS, as it can compromise their ability to reliably distinguish between lawful and unlawful targets. The ICRC report on *Autonomy, artificial intelligence and robotics:*

[369] Ibid., p. 60.
[370] ICRC, *Artificial intelligence and machine in armed conflict: A human-centred approach,* p. 476.
[371] V. Boulanin and M. Verburggen, op. cit., p. 17.
[372] Ibid., p. 16.

Technical aspects of human control identifies several forms of bias that can arise in the development and deployment of AWS.[373] These can be grouped into two broad categories: data-related bias and context-related bias.

Regarding data-related bias, the first and most common type of bias in ML systems is training data bias, which arises when the datasets used to train the system are incomplete, of poor quality, or lack diversity. As a result, the model may fail to perform reliably or relflect real-world complexity, as it cannot account for the full range of situations it may encounter when deployed.[374] Another form is algorithmic focus bias, which arises when a system assigns disproportionate weight to certain inputs while ignoring others, resulting in flawed or unsupported conclusions that do not accurately reflect the data as a whole.[375]

---

[373] ICRC, *Autonomy, artificial intelligence and robotics: Technical aspects of human control*, op. cit., p. 18.

[374] The UNIDIR identifies this bias as "the use of inapproriate training data"; see UNIDIR, *Algorithmic Bias and the Weaponization of Increasingly Autonomous Technologies: A primer*, UNIDIR Resources, nº. 9, 2018, p. 3, accessible at: https://unidir.org/wp-content/uploads/2023/05/algorithmic-bias-and-the-weaponization-of-increasingly-autonomous-technologies-en-720.pdf. ; For instance, an AWS trained mostly on combat data from desert environment, might not correctly recognize people, vehicles, or buildings if it is later deployed in an urban or a mountainous area, simply because it has not seen this environment and its components before. As a result, it might mistakenly classify a civilian vehicle as a military target.

[375] UNIDIR, *Algorithmic Bias and the Weaponization of Increasingly Autonomous Technologies: A primer*. op.cit., ; the Report identifies this

A third type of bias is algorithmic processing bias, which refers to bias introduced by the algorithm itself or by developers — intentionally or not — often through built-in assumptions aimed at compensating for other limitations or to prevent other biases.[376]

Turning to context-related bias, emergent bias arises from the context in which the algorithm is used, rather than to its initial design or training data. It develops during the system's interaction with its environment and only becomes apparent once the system is operational.[377] Transfer context bias occurs when a system is deployed in an environment significantly

bias as "inappropriate focus". For example, a system could wrongfully target a civilian aid worker or a refugee who carries a large bag, because it has been trained to prioritize people carrying large shaped objects, as an indication for carrying weapons; or it can associate specific clothing or movement patterns with combatant behavior that can potentially result in an unlawful attack on a civilian.

[376] Ibid., p. 4. For example, in an effort to prevent the system from being too sensitive to irrelevant data, developers might limit the weight given to certain variables. However, this limitation can lead to the system ignoring important contextual information, resulting in flawed or oversimplified decisions. In the context of AWS, this might mean failing to account to subtle indicators that distinguish a combatant from a *hors de combat*.

[377] ICRC, *Autonomy, artificial intelligence and robotics: Technical aspects of human control*, op. cit., p. 18. For example, a system might start making unexpected and unpredictable decisions if it has the capabilities to adapt its behaviour over time based on feedback from its environment. It might change how it classifies threats after seeing certain patterns. This type of bias is not built into the system from the start but develops as it interacts with the external world.

diffirent from the one it was designed and tested for, potentially leading to failures or unpredictable behavior. [378] Lastly, interpretation bias arises when the operator misreads or over-trusts the system's output, particularly when that output does not align with the type or clarity of information needed to make an informed decision.[379]

All of these types of bias are dangerous — particularly, if they involve life-and-death decisions. The landscape of potential biases supports that AWS, despite the possibility of not being considered unlawful *per se* or by design, will, at least — in *some* cases — violate IHL rules, particularly the targeting law, by their inherent technological limitations.

In this regard, the ICRC notes that the inherent unpredictability, lack of explainability, and potential bias introduced by machine learning raise serious doubts about

[378] UNIDIR, *Algorithmic Bias and the Weaponization of Increasingly Autonomous Technologies: A primer*, op. cit., pp. 4-5. For example, a system trained on conventional war settings where enemies wear uniforms and follow certain patterns, might, if used in a guerilla warfare context, where fighters may dress like civilians, misclassify targets and fail to distinguish between combatants and non-combatants.

[379] Ibid., pp. 5-6. For instance, if the system suggests that a target has an 80% likelihood of being hostile, the operator might treat that number as certainty — even though there is still a high chance that the target is a civilian. This can potentially lead to unlawful attacks, especially when decisions are made quickly or under pressure even when a human is "on-the-loop".

whether such systems can be lawfully used to perform critical functions like target selection and engagement.[380] These issues go beyond technical design — they call for a human-centered approach that preserves human judgment and accountability in life-and-death decisions.[381]

SECTION 2– EXISTING AUTONOMOUS WEAPON SYSTEMS AND THEIR OPERATIONAL DEPLOYMENT

It was previously established that, from a human-centered approach, there is a conceptual difference between AWS in the broad sense — which includes semi-autonomous weapons, supervised autonomous weapons, and fully autonomous weapons — and AWS in the narrow sense, understood as those that function entirely autonomously without human control after activation. To be considered an AWS in the narrow sense, the human must be entirely removed from both loops: the internal Sense-Think/Decide-Act loop and the external OODA loop. In such a configuration, the human's role is reduced to that of an observer, with no capacity to influence the weapon's actions once it has been deployed on the battlefield.

---

[380] ICRC, *Autonomy, artificial intelligence and robotics: Technical aspects of human control*, op. cit., p. 19.
[381] Ibidem.

This type of configuration is particularly problematic because the weapon substitutes the human to such an extent that it has been compared to a combatant,[382] or at the very least, has raised debates about whether it should be considered a traditional weapon or whether it exists in a grey area not yet fully addressed by legal norms. War has been, and still remains, a human endeavor, thus removing the human element from targeting decisions raises significant ethical and legal concerns.

This is why, from a task-centric approach, functions such as targeting and engaging are particularly problematic. Targeting, in particular, is the most debated function, as it requires the system to identify its targets accurately, distinguish lawful from unlawful targets, assess the proportionality of attacking each target, and take all feasible precautions to minimize collateral harm to protected persons and objects. Although technically feasible to a certain extent — and arguably even better performed by machines than humans — targeting law was conceived for human combatants and commanders. Whether this historical fact is still relevant, and whether IHL can adapt to encompass weapons undertaking cognitive tasks traditionally assigned to human combatants and commanders,

[382] See Chapter 2, Section 1: The Legal Nature of Autonomous Weapon Systems.

remains a debated issue. What matters, however, is that, as Rain Liivoja notes "[t]he bulk of the law of war is technology-indifferent."[383] It can — at least theoretically and normatively — stretch to encompass emerging technologies in the context of warfare. It establishes objective parameters — obligations and limitations — that, when respected, ensure compliance with IHL regardless of whether the decision to use force is made by a human or a machine.[384]

The problem arises when these obligations are breached: who can be held responsible? The concept of individual criminal responsibility under ICL cannot be extended to machines, however sophisticated or "intelligent" they may become, because intent — a manifestation of agency — can only be established in relation to a human being.

This is where the technology-centric approach becomes increasingly relevant. AWS, in the narrow sense, are technically more sophisticated than automated systems. This sophistication is demonstrated by cognitive-like capabilities that enable them to perform tasks independently, in what appears to be making a

[383] R. Liivoja, *Technological change and the evolution of the law of war*, International Review of the Red Cross, vol. 97, nº. 900, 2015, p. 1168.
[384] Ibidem.; "The law of war governs the conduct of hostilities and offers protection to persons not taking part in hostilities–all quite irrespecive of the means and methods of warfare the belligerents adopt and other technology they use".

"choice" or, as often termed, "decision-making" — even though they are merely executing pre-programmed instructions. If their programming follows a deterministic model, their actions remain explainable to developers and predictable to operators and commanders. This facilitates the attribution of responsibility in cases of intentional violations of targeting rules. Conversely, if their programming is based on machine learning algorithms — particularly deep neural networks and reinforcement learning — the situation becomes more complex. Their black box nature makes them incomprehensible even to developers, and their behavior inherently unpredictable, since they learn both from external environments and from internal data without their operators being able to fully control or predict what they will learn or how they will act in all operational scenarios.

When combining the limitations raised by each approach, multiple violation scenarios can be envisioned. Their likelihood is as plausible as the possibility that AWS might be more compliant with IHL than human operators. That said, many existing weapon systems do manifest autonomous characteristics, particularly from a task-centered perspective. Some systems can indeed select and engage targets

autonomously, albeit currently under human supervision;[385] others are capable of completing the entire targeting cycle on their own but require human validation before using force.[386]

Such systems — despite not currently qualifying as AWS in the narrow sense — benefit from the loophole of "nominal human intervention"[387] — identified by the State of Palestine in its formal submission to the Secretary-General — as a way out of the "without human intervention" definitional element of AWS.

The submission notes that:

> [I]f we accept the term "without human intervention" without further clarification, it could create a significant loophole in the definition. In theory, all it would require for a system to fall outside the scope of the framework of [AWS] is a single human input after activation of the system.[388]

[385] For example the MK15– Phalanx Close-In Weapon System (CIWS) is "capable of autonomously performing its own search, detect, evaluation, track, engage and kill assessment functions", see: U.S. Navy, *MK15 Phalanx Close-In Weapon System (CIWS)*, Navy.mil, Fact Files, 2021, accessible at: https://www.navy.mil/resources/fact-files/display-factfiles/article/2167831/mk-15-phalanx-close-in-weapon-system-ciws/.

[386] For example the Super aEgis II sentry gun is a turret-based weapon that autonomously detects, tracks and targets potential threats using thermal imaging and surveillance sensors, it supports two firing modes: manual and autonomous, albeit currently requiring human authorization before engaging lethal force, see: Army Guide, *Super aEgis II*, n.d., accessible at: https://www.army-guide.com/eng/product4914.html.

[387] A. Guterres, A/79/88, op. cit., p. 116.

[388] Ibidem.

It further observes that

> It is apparent from analysis of vast range of weapons systems incorporating autonomy, that almost all of them allow a human to engage with the system with a "nominal human input" after the system's activation. Despite being "nominal", weapons designers and manufacturers are able to avoid the system being labelled as an [AWS] by suggesting that an intervention can be made after the system's activation, thereby taking it out of the scope of [AWS].

This observation, when considered alongside the arguments of AWS proponents, and the current deployment of systems featuring increasing degrees of autonomy in their functioning, suggest a potential shift toward autonomous warfare — even if, for now, the prevailing consensus is to maintain the human element, at least within the ODDA loop. However, this political will is not fixed in stone and may change in the future.

Accordingly, the following section will present examples of currently existing weapon systems that plausibly have the potential to evolve in the future toward functioning in fully autonomous modes (A), as well as real armed conflict scenarios where reliance on AI has already enhanced effective autonomy over targeting and engagement processes (B) to illustrate the trajectory of this technological evolution.

A. EXAMPLES OF EXISTING AUTONOMOUS WEAPON SYSTEMS

Autonomous systems exist for multiple roles in contemporary warfare, ranging from intelligence, surveillance, and reconnaissance (ISR) to logistical support,[389] electronic warfare,[390] and direct combat operations.[391] These systems vary widely in terms of their function, complexity, degree of autonomy, and nature of the task rendered autonomous. Some are designed to enhance situational awareness by gathering and processing battlefield information; others assist with communications, mobility, or decision support.[392] Among these, are AWS — additionally characterized is by the fact that the system is armed and capable of exerting force.

AWS may be divided according to their operational roles into defensive systems, which are primarily designed to detect

[389] V. Boulanin and M. Verburggen, op. cit., pp. 20-21.
[390] M. Thompson, *Beyond The Battlefield: Navigating The Future of AI and Autonomous Systems in Electronic Warfare*, The Journal of Electromagnetic Dominance, 2024, accessible at: https://www.jedonline.com/2024/05/06/beyond-the-battlefield-navigating-the-future-of-ai-and-autonomous-systems-in-electronic-warfare/.
[391] S. Pal, *Autonomous Combat Systems: Challenges and Opportunities in Land, Air, and Sea*, Medium, 2023, accessible at: https://medium.com/@siam_VIT-B/autonomous-combat-systems-challenges-and-opportunities-in-land-air-and-sea-74d554a926a.
[392] Ibidem.

and neutralize incoming threats to fixed assets or personnel, and offensive systems, which are designed to actively seek out and attack enemy forces or infrastructure. For the purposes of this analysis, the focus will be limited to these two categories — defensive and offensive AWS — as they are the most relevant to the legal and ethical issues associated with targeting and the use of force.

Defensive AWS are designed to serve primarily defensive roles, meaning they do not take the initiative to exert force, and operate reactively, engaging only when a threat is identified.[393] Once activated, these systems autonomously detect incoming hostile projectiles — such as rockets or missiles — often within seconds, and far faster than human operators could respond.[394] Their operation is generally confined to narrowly defined parameters and specific trigger conditions, with minimal variability or room for discretion.[395] Until now, existing defensive systems operate under human supervision (human-on-the-loop), meaning that a human operator can monitor their performance and intervene if necessary, but is not directly

[393] Examples of these systems include the Phalanx CIWS (United States) and the Iron Dome (Israel).
[394] P. Scharre, *Army of None*, op. cit., p. 52; V. Boulanin and M. Verburggen, op. cit., p. 37.
[395] V. Boulanin and M. Verburggen, pp. 37-38.

involved in each engagement decision.[396] This predictability and limited scope of action have contributed to their characterization as low-risk applications of autonomy in warfare.[397]

Conversely, offensive AWS can be considered the most controversial types of AWS, as they are designed to take the initiative in applying force. Their mission is to neutralize targets deemed hostile, meaning they proactively seek out and attack enemy forces or assets. To date, these are not reported as widely used. Loitering attack drones are identified as the only real form of offensive autonomous weapons currently deployed.[398] Even these are typically configured in advance by humans, who determine parameters such as the loitering time, the geographical areas of deployment, as well as the category of targets they are authorized to attack.[399]

Despite the importance of this conceptual distinction, it is important to recall that, a weapon is inclusively defined as an

[396] P. Scharre, *Army of None*, pp. 52-53.
[397] A. Guterres, A/79/88/, op. cit., p. 6 §7 "Several States suggested that certain autonomous or automatic anti-aircraft and missile defence systems should not be considered lethal autonomous weapons systems, given their defensive nature and the deterministic, rather than probabilistic, nature of the algorithms used by those systems for the detection and engagement of targets. They noted that such systems had been used for decades without legal controversy".
[398] V. Boulanin and M.Verbruggen, op. cit., p. vii.
[399] Ibidem.

instrument of offensive or defensive combat.[400] This broad definition may create ambiguity for two main reasons. First, in the formulation of legal frameworks, as many states heavily rely on defensive AWS and may strongly resist any attempt to prohibit them.[401] Second, certain systems can be deployed for both offensive and defensive missions, rendering their classification more complex.[402]

Moreover, the nature of the target is a critical factor in evaluating the legal and ethical risks posed by these systems: anti-material AWS (targeting objects such as projectiles or vehicles) generally represent fewer compliance challenges under IHL than anti-personnel AWS, which are subject to stricter rules, as the target is a human being.[403] Additionally, the operational environment also significantly influences the risk profile of AWS. Systems deployed in controlled settings where civilian presence is minimal, are often perceived as less problematic and more suitable for autonomy, particularly when

[400] R. C. Anugrah, *A Defense for Guardian Robots: Are Defensive Autonomous Weapons Systems Justifiable?* Harvard International Law Journal, Online Scholarship, Perspectives, 2024, p. 3.
[401] A. Guterres, A/79/88, op. cit., p. 6 §7.
[402] V. Boulanin and M. Verburggen, op. cit., p. 40 and p. 50.
[403] Ibid., p. 74.

rapid reaction is critical and human reaction times may be insufficient.[404]

Against this complexity, a 2017 study conducted by researchers at the SIPRI examined 381 existing weapon systems featuring varying degrees of autonomy in their functions, in order to map the state of autonomy across the different functions of a weapon system.[405] The researchers noted that beyond navigation, targeting was the most notable application area of autonomy in weapon systems.[406]

The SIPRI study classified systems under review into five categories: (1) air defense systems; (2) active protection systems; (3) robotic sentry weapons; (4) loitering weapons; and

[404] P. . Scharre, *Army of None*, op. cit., p. 52; V. Boulanin and M. Verburggen, op. cit., p. 37.

[405] Ibid., pp. 19-20. The researchers classified the systems studied as follows: (1) Unmanned weapon systems that feature some autonomy in their critical functions–that is, they can autonomously search for, detect, identify, select, track or attack targets. (2) Unmanned weapon systems that do not have autonomy in their critical functions but feature autonomous functions in any of the other capability areas covered by the study–namely mobility, intelligence, interoperability and health management. (3) Unmanned and unarmed military–uses of which include (but are not limited to) intelligence, surveillance and reconnaissance (ISR) missions or logistics (supply) missions–that feature any of the capability areas covered by the study.

[406] Ibid., p. 24. According to the study, in at least 154 systems, autonomy was used to support some, if not all, of the steps of the targeting process (at the tactical level), from identification, tracking, prioritization and selection of targets to, in some cases, target engagement.

(5) guided munitions.[407] However, guided munitions — such as cruise missiles and torpedoes — will be excluded from the present analysis. Although they share the fire-and-forget characteristic with other autonomous systems, they are typically pre-programmed with fixed parameters for target selection and engagement, limiting their operational autonomy once launched. Moreover, as the SIPRI researchers noted, mapping guided munitions would require a separate, dedicated study, due to the breadth of available models.[408] Therefore, this analysis will focus specifically on weapon systems rather than individual munitions.

1. AIR DEFENSE SYSTEMS

Air defense systems are "weapon systems that are specifically designed to nullify or reduce the effectiveness of hostile air action".[409] These include missile defense systems, anti-aircraft systems and close-in weapon systems (CIWSs)[410], all of which use radar to detect and track incoming threats (missiles, rockets, or enemy aircraft) and a computer-controlled

[407] Ibid., p. 36.
[408] Ibid., p. 20.
[409] Ibid., p. 36.
[410] Ibidem.

fire system that can prioritize, select, and where authorized, autonomously attack those threats.[411]

Air defense systems can be differentiated based on several criteria: (1) the range of engagement, (2) the types of targets they can engage, and (3) the type of countermeasures.

Regarding the range of engagement, CIWSs like the *GoalKeeper* (Netherlands) or the *Phalanx* (USA) are designed to defend a limited geographical zone, such as a ship or military base. In contrast, missile defense systems like the *Iron Dome* (Israel) can provide protection over a large geographic area, including borders or cities.[412]

Regarding the types of targets they are authorized to engage, the existing air defense systems are all anti-material (i.e., they are not designed to target people). While many systems target airborne threats, capabilities differ. For instance, the land-based *Centurion C-RAM* (USA) is limited to incoming air projectiles, whereas the naval Phalanx can also engage surface threats like fast-attack crafts.[413] The variation often reflects differing risks of collateral damage, which are typically higher in land operations than at sea.[414]

---

[411] Ibidem.
[412] Ibid., pp. 36-37.
[413] Ibid., p. 37.
[414] Ibidem.

Regarding the type of countermeasures, the majority of air defense systems use *hard-kill* measures to defeat incoming threats, i.e., they fire missiles or bullets to destroy the incoming target.[415] Conversely, other systems can also use *soft-kill* measures that interfere with the threat's tracking and guidance systems using electromagnetic or acoustic disruption.[416]

Their capabilities and performance vary depending on the system. For example, the S-400 Triumf (Russia) can reportedly track over 300 targets and engage 36 simultaneously at distances up to 250 km; or the Rapier (United Kingdom) can launch within six seconds of detecting a target.[417]

Air defense systems are widespread technology: the study identified at least 89 countries having automatic air defense systems and 63 countries deploying more than one type of air defense system.[418] Nevertheless, these systems operate under human supervision — mostly, on a human-on-the-loop mode.

2. ACTIVE PROTECTION SYSTEMS

Active protection systems (APSs) are anti-material defensive weapon systems that are designed to protect armored vehicles against threats such as incoming anti-tank missiles or

[415] Ibidem.
[416] Ibidem.
[417] Ibidem.
[418] Ibidem.

rockets.[419] Functionally, they operate on the same basic principle as air defense systems by combing a sensor — such as radar, IR, or ultraviolet (UV) — with a fire control system that detects, tracks, and classifies incoming threats.[420] Once a threat is assessed, the system then deploys a countermeasure — either hard-kill or soft-kill — at the optimal time and location to neutralize the threat.[421]

The SIPRI study identified 17 APSs, highlighting a growing interest in these systems over the past decade, primarily due to the proliferation of anti-tank guided missiles (ATGMs) and rocket-propelled grenades (RPGs) among non-state armed groups.[422] These threats have significantly challenged the survivability of armored vehicles, prompting militaries to invest in technologies that can counter them more effectively.[423] Nevertheless, APSs have seen only limited use in combat, making their use and the effects that their use might have on civilian and friendly forces little known.[424]

[419] Ibid., p. 41.
[420] Ibidem.
[421] Ibidem.
[422] Ibid., p. 42.
[423] Ibid., p. 41.
[424] Ibid., p. 44.

3. ROBOTIC SENTRY WEAPONS

Robotic sentry weapons are stationary or mobile gun turrets that can automatically detect, track, and potentially engage human targets.[425] Typically deployed for perimeter and border defense, these systems are distinct in that they are often used for anti-personnel purposes — unlike air defense or APSs, which target incoming projectiles.[426] They integrate visual, infrared, and motion-detection sensors with fire-control algorithms to operate with limited or no human intervention.[427]

Although still relatively rare, three notable models have been identified: Samsung's *SGR-A1* (now retired), DODAAM's *Super aEgis II*, both developed by South Korea, and Raphael's *Sentry Tech* developed by Israel.[428]

These systems are primarily used for surveillance and deterrence.[429] However, the mode of target recognition — typically based on motion and heat signatures — raises

[425] Ibidem.
[426] Ibidem.
[427] M. Kashif, M. Arslan, R. Chakma, F. Banoori, A. Al Mamun, G. L. Chakma, *Design and Implementation of Image Capture Sentry Gun Robot*, MATEC Web of Conferences, 160, 06007, 2018, p. 1, accessible at: https://www.matec-conferences.org/articles/matecconf/pdf/2018/19/matecconf_eecr2018_06007.pdf.
[428] V. Boulanin and M. Verburggen, op. cit., p. 44.
[429] Ibid., p. 45.

significant concerns, particularly regarding the distinction between civilians and combatants. In other words, the problem with such systems is that they recognize targets based on heat and motion patterns. They are therefore unable to reliably distinguish between civilian and military human targets.[430] While the SGR-A1 was reportedly able to recognize surrender gestures and motions (such as arms held high to indicate surrender)[431], and the Super aEgis II claims the ability to sense and detect whether a human target is carrying explosives under their clothing[432], these features remain highly controversial and difficult to verify under combat conditions.

In its original design, the Super aEgis II was intended to carry out all steps of the targeting and engagement processes fully autonomously.[433] It was built with a speech interface that allows it to interrogate and warn detected targets. However, due to concerns over the possibility of erroneous engagements, the system was revised to allow three modes of human involvement:

- Human-in-the-loop (the human operator must enter a password to unlock the robot's firing ability and give the manual input that permits the robot to shoot);
- Human-on- the-loop (a human operator supervises and can override the actions of the system); and

[430] Ibidem.
[431] Ibidem.
[432] Ibid., p. 46.
[433] Ibidem.

- Human-out-of-the-loop (the system is fully autonomous and not supervised in real time by a human operator).[434]

Regarding their current operational mode, robotic sentry weapons are controlled by a human once targets are detected. Some models require a minimum of two people to operate each robot, one operator and one commander.[435] However, since they have not been widely used in combat, their deployment raises significant legal concerns — especially with regard to distinction and proportionality. Some argue that their use in highly controlled zones with little to no civilian presence could reduce the risk of unlawful harm, though this remains a contested point.[436]

4. LOITERING WEAPONS

Loitering weapons — also referred to as loitering munitions or *suicide drones* — are a hybrid type of weapon system that fits a niche between guided munitions and unmaned combat aerial systems (UCASs).[437] They combine the purpose and attack mode of guided munitions with the maneuverability

[434] Ibidem.
[435] Ibid., p. 47.
[436] Ibidem.
[437] Ibid., p. 50.

of UCAs.[438] This means that they can loiter in a designated area, for an extended period of time, to find suitable targets on the ground, at which point they dive toward the target and detonate upon impact.

The SIPRI study notes that their operational utility lies in two key features: (1) they are not aimed at a predefined target but rather a target area (2) they are disposable by design, meaning they are not intended for retrieval after mission completion.[439] This makes them well suited for offensive and defensive missions, particularly those that might be deemed dangerous or risky for other types of unmanned or manned systems or where reusable systems would be unsafe or impractical.[440] Additionally, loitering munitions come in all sizes and shapes, and vary in loitering time, payload, human-machine command-and-control architecture, and recoverability.[441]

Although the large majority of existing loitering weapons operate remotely by human controllers, a growing number are being equipped with increasingly autonomous capabilities. According to the SIPRI dataset, only four systems have been

[438] Ibidem.
[439] Ibidem.
[440] Ibid., pp. 50-51.
[441] Ibid., pp. 52-53.

confirmed as capable of carrying out the entire targeting cycle — find, track, and attack targets in complete autonomy once launched: the *Orbiter 1K 'Kingfisher'*, the *Harpy*, the *Harop* and the *Harpy NG*, all developed by Israel.[442]

The Harpy, developed by Israel in the 1990s, is the oldest operational loitering munition and is designed to function in complete autonomy.[443] It was specifically engineered for Suppression of Enemy Air Defenses (SEAD) missions and operates similarly to an anti-radiation missile, autonomously detecting and striking radar-emitting targets.[444] Its successors — the Harop and Harpy NG — as well as the Orbiter 1K, represent more advanced iterations of the same concept. These newer systems include both fully autonomous and human-in-the-loop modes.[445] While the autonomous mode appears to be reserved primarily for SEAD missions, the human-in-the-loop configuration is generally preferred for high-value targets, such as armored vehicles.[446] In such operations, the loitering munition uses optical and infrared sensors to identify and

[442] Ibid., p. 53.
[443] Ibid., p. 54.
[444] Ibidem.
[445] Ibidem.
[446] Ibidem.

monitor potential targets, while a human operator retains the ability to abort the mission until just moments before impact.[447]

The preceding panorama of existing AWS — albeit not exhaustive — provides a typology of current technologies and capabilities, however, it remains incomplete without considering their actual use in the battlefields. Accordingly, the analysis now turns to four recent armed conflicts that offer illustrative examples of the growing integration of autonomous functions and AI into deployed weapon systems, and the extent to which this reflects a broader trajectory toward autonomous warfare.

B. AUTONOMOUS WEAPON SYSTEMS IN RECENT ARMED CONFLICTS

Under Article 2(4) of the United Nations Charter, the threat or use of force in international relations is strictly prohibited, with only limited exceptions permitted under international law. As a result, most armed conflicts in the post-Charter era have occurred within state borders and have taken the form of non-international armed conflicts (NIACs), rather than international armed conflicts (IACs). However, the recent resurgence of large-scale IACs has accelerated the proliferation and

[447] Ibidem.

operational testing of new military technologies, including AWS and AI-enabled targeting systems.

Four conflicts in particular — (1) Libya (NIAC-2020), (2) Nagorno-Karabakh (2020), (3) Ukraine (2022), and (4) Gaza (2023) — offer key illustrations, not only of the deterioration in the global security, but also of the increased use of autonomy in warfare. Crucially, these cases demonstrate that autonomy in weapons is no longer limited to theoretical or experimental settings, but is now being deployed in real battlefields, raising serious challenges for compliance with IHL and highlighting ethical concerns associated with so-called "Killer Robots."

1. THE ARMED CONFLICT IN LIBYA (2020)

After the fall of Muammar Gaddafi in 2011, Libya fractured into rival governments and militias. The country has since experienced what is commonly referred to as the *Libyan Second Civil War*, which lasted from 2014 to 2020 and was primarily opposing two dominant factions: the UN-recognized Government of National Accord (GNA), based in Tripoli, and the Libyan National Army (LNA), led by General Khalifa Haftar, based in the east of the country.[448] Between 2014 and

[448] See more on the Libyan civil war: H. Anjum, *Second Libyan Civil War (2014-2020): Causes and Impacts*, n.p., 2022, accessible at: https://www.researchgate.net/publication/366445100_SECOND_LIBYAN_CIVIL_WAR_2014-2020_CAUSES_AND_IMPACTS; Center for

2019, the conflict was marked by periods of intense fighting, failed ceasefires and unproductive political negotiations. Despite the 2015 UN-brokered *Libyan Political Agreement*,[449] attempts to unify Libya's fragmented political actors under a single authority were unsuccessful. Rival factions continued to expand influence through the establishment of parallel institutions, seeking external support, and recurring military operations.[450]

On 4 April 2019, General Haftar (LNA) launched a major offensive to seize Tripoli.[451] His forces, known as the Haftar Affiliated Forces (HAF), advanced rapidly, and for over a year,

---

Preventive Action, *Civil Conflict in Libya*, Global Conflict Tracker, 2024, accessible at: https://www.cfr.org/global-conflict-tracker/conflict/civil-war-libya ; M. Cruickshank, Libya's Second Civil War: How did it come to this? Conflict News, 2014, accessible at: https://web.archive.org/web/20150320232806/http://www.conflict-news.com/libyas-second-civil-war-how-did-it-come-to-this/.

[449] United Nations Support Mission in Libya (UNSMIL), *The Libyan Political Agreement*, signed in Skhirat, Morocco on 17 December 2015, accessible at: https://unsmil.unmissions.org/sites/default/files/Libyan%20Political%20Agreement%20-%20ENG%20.pdf.

[450] Center for Preventive Action, *Civil Conflict in Libya,* op. cit.

[451] AlJazeera, *Timeline: Haftar's months-long offensive to seize Tripoli*, 19 Feb 2020, accessible at: https://www.aljazeera.com/news/2020/2/19/timeline-haftars-months-long-offensive-to-seize-tripoli; AlJazeera, *'Brief skirmish' near Libya's Tripoli as Haftar's LNA heads west*, 4 Apr 2019, accessible at: https://www.aljazeera.com/news/2019/4/4/brief-skirmish-near-libyas-tripoli-as-haftars-lna-heads-west.

the fighting concentrated around the capital.[452] In March 2020, the GNA launched "*Operation Peace Storm"*, shifting from defense to offense.[453] This marked a turning point in the conflict due to the increased deployment of Turkish-supplied drones, loitering munitions, and advanced electronic warfare systems.[454]

Among these weapon systems was the STM *Kargu-2,* a Turkish-manufactured quadcopter drone capable of operating both manually and autonomously.[455] It is reported to use "machine learning algorithms embedded on the platform" and "real-time image processing" to identify and engage targets.[456] The drone can be used in a fire-and-forget mode or in a fully autonomous "fire, forget, and find" capability.[457]

---

[452] Ibidem.; Center for Preventive Action, *Civil Conflict in Libya,* op. cit.
[453] UN Security Council, *Final report of the Panel of Experts on Libya established pursuant to Security Council resolution 1973*, S/2021/229, p. 17 § 63; The Libya Observer, *Libyan Army launches Operation Peace Storm against Haftar's attacks on civilians*, 25 March 2020, accessible at: https://libyaobserver.ly/news/libyan-army-launches-operation-peace-storm-against-haftars-attacks-civilians.
[454] A. Thomas, *The Turkey-UAE race to the bottom in Libya: a prelude to escalation,* Fondation pour la Recherche Stratégique, Recherches & Documents, nº 8/2020, pp. 5-7 and pp. 8-11.
[455] H. Nasu, *The Kargu-2 Autonomous Attack Drone: Legal & Ethical Dimensions*, Lieber Institute West Point, 2021, accessible at: https://lieber.westpoint.edu/kargu-2-autonomous-attack-drone-legal-ethical/.
[456] Ibidem.
[457] UN Security Council, S/2021/229, op. cit., p. 17 § 63; see also: ICRC, *Libya: Use of Lethal Autonomous Weapon Systems*, ICRC Casebook, 2021,

In a 548-page report to the UN Security Council, the *Panel of Experts on Libya established by the SC resolution 1973 (2011)*, reported that the Kargu-2 was used to track and strike retreating HAF forces without any real-time human control, potentially marking the first recorded battlefield use of a *fully* autonomous weapon system.

The report stated that

> Logistics convoys and retreating HAF were subsequently hunted down and remotely engaged by the unmanned combat aerial vehicles or the lethal autonomous weapons systems such as the STM Kargu-2 (see annex 30) and other loitering munitions.*The lethal autonomous weapons systems were programmed to attack targets without requiring data connectivity between the operator and the munition: in effect, a true "fire, forget and find" capability*.[458]
>
> [...]
>
> Once in retreat, they were subject to continual harassment from the unmanned combat aerial vehicles and lethal autonomous weapons systems [...]. These suffered significant casualties [...][459]

Although the Panel of Experts' report does not confirm whether any fatalities resulted from the attack,[460] it illustrates

accessible at: https://casebook.icrc.org/case-study/libya-use-lethal-autonomous-weapon-systems.

[458] UN Security Council, S/2021/229, op. cit., p. 17, §63; *Italic* added.

[459] Ibidem., §64.

[460] ICRC, *Libya: Use of Lethal Autonomous Weapon Systems,* op. cit., p. 3.

that legal and humanitarian concerns extend beyond the mere question of whether the autonomous system has killed. This deployment raises significant concerns under IHL, particularly with regard to the principle of distinction, which requires that attacks be directed only against combatants and military objectives, excluding civilians and those *hors de combat* from the scope of lawful attacks. The autonomous use of Kargu-2 against retreating forces raises questions as to whether the drone could have adequately verified the lawful status of its targets before engagement.[461]

Furthermore, this reported use of the Kargu-2 in a "fire, forget, and find" mode represents a significant shift from the original paradigms of human-in-the-loop and human-on-the-loop control, confirming the significant concern over deploying AWS without meaningful human control. Nonetheless, while the conflict in Libya raised alarm from a human-centered perspective — particularly due to the use of AWS without real-time human control — the conflict in Nagorno-Karabakh, by contrast, attracted military interest for its pioneering use of

[461] H. Nasu, op. cit., accessible at: https://lieber.westpoint.edu/kargu-2-autonomous-attack-drone-legal-ethical/. As Hitoshi Nasu observes, "[t]he employment of autonomous systems [...] without appropriate capabilities to identify and spare those who are recognized as hors de combat raises legitimate issues regarding the systems' ability to comply with the law of armed conflict."

loitering munitions and swarm-like tactics — reflecting a more technology-centered perspective.

2. THE ARMED CONFLICT IN NAGORNO-KARABAKH (2020)

Arguably described as "the first drone war"[462] in history, the Nagorno-Karabakh conflict between Azerbaijan and Armenia — which lasted 44 days and was briefly suspended by a Russian brokered ceasefire — highlighted how advanced weapon systems can provide tactical superiority, particularly having resulted in the reclamation of significant territories by Azerbaijan.[463]

To provide context, Nagorno-Karabakh is long disputed region — especially since the fall of the USSR — that was officially part of Azerbaijan but has been *de facto* governed by

[462] L. Wilmes and R.V. Waas, *Understanding Arms Races for Autonomous Military Capabilities Using a System Dynamics Simulation Model*, Nato STO Review Spring 2024, p. 2, accessible at: https://review.sto.nato.int/images/Papers/Peer_Review_Journal_4_Spring_2024_21-Wilmes.pdf; see also: T. Kuzio, *Western Weapons Made the Difference in Ukraine and the Second Karabakh War*, Geopolitical Monitor, Opinion, 2024, accessible at: https://www.geopoliticalmonitor.com/western-weapons-made-the-difference-in-ukraine-and-the-second-karabakh-war/.

[463] See G. Angelov, *Military Implications of the Nagorno-Karabkh Conflict: Tactics and Technologies*, Information & Security Journal, vol. 51, 2022, p. 49-55, accessible at: https://isij.eu/system/files/download-count/2023-01/5104_nagorno-karabakh.pdf

ethnic Armenian forces since the early 1990s.[464] Although not the only armed conflict between the two states over this region,[465] the 2020 war was particularly noteworthy because it was characterized by a rapid Azerbaijani offensive, backed by Turkish and Israeli military technologies.[466] In particular, it saw the increased use of unmanned combat air vehicles (UCAVs) and loitering munitions.

Azerbaijan's military strategy relied heavily on three principal systems: the Turkish *Bayraktar TB2* (armed UCAV), the Israeli *IAI Harop* and *Orbiter 1K* loitering munitions. The Bayraktar TB2 was used for both ISR missions and precision-

[464] D. Khachatryan, *Complete Defeat and the End of the Non-Recognized State of Nagorno-Karabak*, Lieber Institute West Point, Articles of War, 2024, accessible at: https://lieber.westpoint.edu/complete-defeat-end-non-recognized-state-nagorno-karabakh/; S. Roblin, *What Open Source Evidence Tells Us About The Nagorno-Karabakh War*, Forbes, 2020, accessible at: https://www.forbes.com/sites/sebastienroblin/2020/10/23/what-open-source-evidence-tells-us-about-the-nagorno-karabakh-war/.

[465] C. Whelan, *The 2020 Nagorno Karabakh War: Unmanned Combat Aerial Vehicles in Modern Warfare*, Air and Space Power Review, vol. 24 no. 2, 2023, pp. 52-54.

[466] See P. Iddon, *Turkey and Israel Upgrade Azerbaijan's Russian Military Hardware*, Forbes, 2024, accessible at: https://www.forbes.com/sites/pauliddon/2024/10/09/turkey-and-israel-upgrade-azerbaijans-russian-military-hardware/; S. Shaikh and W. Rumbaugh, *The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense*, Center for Strategic & International Studies, 2020, accessible at: https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense.

guided strikes using MAM-L munitions.[467] Meanwhile, the Harop and Orbiter 1K systems were deployed to destroy high-value assets such as air defense radars, armored vehicles, and artillery units.[468] These systems were particularly effective against static and signal-emitting targets, allowing Azerbaijan to carry out SEAD operations with minimal risk to its soldiers.[469]

The combination of these three systems allowed Azerbaijan to maintain continuous aerial presence and pressure over the battlefield creating an overwhelming tempo of operations that were challenging to counter by the Armenian forces. Analysts confirmed the destruction and/or seizing of hundreds of Armenian military assets — including tanks and electronic warfare units — resulting in Armenian loss of military equipment worth at least $3.8 billion.[470]

---

[467] J. Postma, *Drones over Nagorno-Karabakh: A glimpse at the future of war?* JSTOR, 2021, pp. 15-16, accessible at: https://www.jstor.org/stable/pdf/48638213.pdf?refreqid=fastly-default%3A9dd091f496d7581327df34bc1a29bc26&ab_segments=&initiator=&acceptTC=1

[468] Ibid., p. 16.

[469] Ibidem.

[470] Top War, *The losses of military equipment of the Armenian Armed Forces in Nagorno-Karabakh assessed in Baku*, Military Review News, citing Ayaz Museibov, Head of the department of the Center for Analysis and Comminication of Economic Reforms (CACER) of Azerbaijan, 2 Dec. 2020, accessible at: https://en.topwar.ru/177706-v-baku-ocenili-poteri-voennoj-tehniki-vs-armenii-vo-vremja-vojny-v-nagornom-karabahe.html.

While most of these targets were reportedly lawful military targets,[471] Human Rights Watch documented repeated strikes by Azerbaijani forces on dual-use infrastructure and civilian areas far from the front lines, as well as the use of cluster munitions without a fixed military target, thereby violating the principles of distinction and proportionality.[472]

The Nagorno-Karabakh conflict demonstrated how the combined use of conventional and autonomous weapons can alter both the conduct and outcome of hostilities. Despite reported IHL violations, these technologies enabled Azerbaijan to secure a clear military advantage. They also contributed to a growing trend in contemporary armed conflicts, where the demonstrated capabilities of weapon systems to identify and engage high-value and protected targets, have prompted other militaries to rely more on such technologies. Particularly, this trend intensified in the armed conflict in Ukraine, following the full-scale invasion by the Russian Federation in 2022.

---

[471] Human Rights Watch, *Azerbaijan: Unlawful Strikes in Nagorno-Karabakh Investigate Alleged Indiscriminate Attacks, Use of Explosive Weapons*, Report, 2020, p. 4, accessible at: https://www.hrw.org/news/2020/12/11/azerbaijan-unlawful-strikes-nagorno-karabakh; see also: BBC, *Nagorno-Karabakh: President Ilham Aliyev speaks to the BBC*, Televised Interview, 9 Nov. 2020, accessible at: https://www.bbc.com/news/av/world-europe-54865589.

[472] Human Rights Watch, *Azerbaijan: Unlawful Strikes in Nagorno-Karabakh*, op. cit., p. 3.

3. THE ARMED CONFLICT IN UKRAINE (2022-ONGOING)

Another inheritance of the USSR's dissolution is the Russian Ukrainian conflict, which intensified in 2014 when Russia annexed Crimea, and erupted into a war in early 2022, when Russia launched a full-scale invasion of Ukraine, marking the first large scale military offensive in Europe since the Second World War (WWII).[473]

The ongoing war has been characterized by the widespread use of AI-enhanced systems, and semi-autonomous platforms, which were used for ISR, targeting and direct attack missions. Ukraine, in particular, openly embraced the use of AWS as part of its military defense strategy.[474] In order to compensate for the numerical disadvantage in comparison to its Russian adversary, and to distance their human soldiers from the front lines of fire, Ukraine relies heavily on domestic and foreign-supplied AWS

[473] For the root causes of the conflict and its chronological development see: S. Demedziuk, *The New Dimension of War – The Ukraine Conflict*, Security and Defence Quarterly, 14(1), n.d., accessible at: https://securityanddefence.pl/pdf-105406-36134?filename=36134.pdf.

[474] K. Bondar, *Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare*, Report, Center for Strategic & International Studies, 2025, p. 1, accessible at: https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare#h2-introduction.

as a force-multiplier.[475] In 2024, Ukrainian factories fabricated nearly two million drones of all classes,[476] with an announcement made by President Volodymyr Zelensky that "Ukraine's defense industry had significantly scaled up its capabilities, reaching an annual production capacity of up to four million drone."[477] In addition to its domestic production, Ukraine procured 10,000 drones equipped with artificial intelligence in 2024, representing 0.5% of the total number of drones contracted.[478]

This trend was expected to accelerate in 2025: Ukraine's Minister of Digital Transformation predicted that 2025 "will significantly increase the percentage of autonomous drones with targeting. We might see the first real drone swarm uses, though

[475] Ibid., p. 7 and p. 10.
[476] Ibidem.; the report notes that according to a statement by Ukraine Minister of Defence, Ukranian defense companies manufactured and assembled more than 1.5 million FPV (First Person View) drones. They also produced other advanced platforms, including strike quadcopter bombers, kamikaze drone, winged reconnaissance drones, and long-range deep-strike drones. It adds that over all, Ukraine produced approximately 2 million drones in 2024.
[477] Reuters, *Ukraine ramps up arms production, can produce 4 million drones a year, Zelensky says*, 2 October 2024, accessible at: https://www.reuters.com/world/europe/ukraine-ramps-up-arms-production-can-produce-4-million-drones-year-zelenskiy-2024-10-02/.
[478] S. J. Freedberg JR, *Trained on classified battlefield data, AI multiplies effectiveness of Ukraine's drones*: *Report*, 2025, accessible at: https://breakingdefense.com/2025/03/trained-on-classified-battlefield-data-ai-multiplies-effectiveness-of-ukraines-drones-report/.

not on a massive scale. The first steps will happen".[479] The objective is to increase the percentage of AI-equipped drones from 0.5 to 50%.[480]

However, it is important to note that Ukrainian military uses the term AWS interchangeably with unmanned systems or platforms equipped with basic autonomous functions such as navigation or targeting.[481] As such, these declarations are to be considered with caution because many of these systems — while they may operate without direct human control — they frequently do not perform the entire process of finding, selecting, and engaging targets independently.[482]

Yet, the terminological discrepancy does not alter the fact that Ukraine is indeed pursuing full autonomy[483] and leveraging technological advances to compensate for vulnerabilities and

[479] S. Bendett and D. Kirichenko, *Ukraine Symposium – The Continuing Autonomous Arms Race*, Lieber Institute West Point, 2025, accessible at: https://lieber.westpoint.edu/continuing-autonomous-arms-race/.
[480] S. J. Freedberg JR, op. cit.
[481] K. Bondar, op. cit., p. 6.
[482] Ibid., pp. 6-7.
[483] Ukranian Deputy Prime Minister Mykhailo Fedorov's declared that fully autonomous weapon systems are "a logical and inevitable next step" in weapons development. See Associated Press News, *Drone advances in Ukraine could bring dawn of killer robots*, 9 May 2023, accessible at: https://apnews.com/article/russia-ukraine-war-drone-advances-6591dc69a4bf2081dcdd265e1c986203.

achieve technological supremacy over its Russian adversary.[484] This observation prompted analysts to identify Ukraine as a "laboratory"[485] or a "testing ground for the future of warfare",[486] which is "laying the groundwork for a future autonomous battlefield environment".[487]

An exhaustive analysis of weapons systems used in this conflict is beyond the scope of the study; however, light will be shed only on selected weapon systems that were employed by Ukraine and Russia,[488] some of which have reportedly resulted in violations of IHL.[489]

---

[484] K. Bondar, op. cit., p. 7; see also: D. Kirichenko, *Drone superpower: Ukrainian innovation offers lessons for NATO*, Atlantic Council Blog, 2025, accessible at: https://www.atlanticcouncil.org/blogs/ukrainealert/drone-superpower-ukrainian-wartime-innovation-offers-lessons-for-nato/.

[485] CNN, *How Ukraine became a testbed for Western weapons and battlefield innovation*, 15 Jan 2023, accessible at: https://edition.cnn.com/2023/01/15/politics/ukraine-russia-war-weapons-lab.

[486] S. Bendett and D. Kirichenko, op. cit.

[487] K. Bondar, op. cit., p. 11.

[488] Automated Decision Research, *Weapons Systems with autonomous functions used in Ukraine*, n.d., accessible at: https://automatedresearch.org/news/weapons-systems-with-autonomous-functions-used-in-ukraine/.

[489] S. Sotoudehfar, *Drone on the frontline: Charting the use of drones in the Russo-Ukrainian Conflict and how their use may be violating international humanitarian law*, International and Comparative Law Review, vol. 23, no. 2, 2023, accessible at: https://sciendo.com/article/10.2478/iclr-2023-0018 .

Ukraine notably integrated foreign-supplied AWS, such as the Turkish Bayraktar TB2 drones, previously alleged to have been used autonomously in Libya. These drones feature autonomous capabilities, including target acquisition through onboard laser designators, and can execute precise strikes independently once approved by operators.[490] Data from the Ukrainian ministries indicate that the deployment of TB2 drones resulted in the destruction of various Russian military assets, including tanks, armored vehicles, anti-craft systems and electronic warfare systems.[491]

Additionally, Ukraine employed the American *Switchblade* and *Phoenix Ghost* loitering munitions. Although details on the Phoenix Ghost remain limited, it reportedly mirrors Switchblade functionalities: offering autonomous navigation and advanced target recognition capabilities.[492]

---

[490] Automated Decision Research, op. cit.

[491] O. Sapwood, *In the south of Ukraine, the Bayraktar TB2 drone neutralized the tanks of the Russian Federation*, MILITARNY, 2022, accessible at: https://militarnyi.com/en/news/in-the-south-of-ukraine-the-bayraktar-tb2-drone-neutralized-the-tanks-of-the-russian-federation/; Army Recognition, *Ukrainian Drones Destroyed 88 Russian Tanks This Month in Two-Week Technological Blitz*, 2024, accessible at: https://armyrecognition.com/focus-analysis-conflicts/army/conflicts-in-the-world/russia-ukraine-war-2022/ukrainian-drones-destroyed-88-russian-tanks-this-month-in-two-week-technological-blitz?highlight=WyJydXNzaWEiXQ%3D%3D.

[492] Automated Decision Research, op. cit.; see also: AVINC, *Switchblade 300 Block 20*, accessible at: https://www.avinc.com/lms/switchblade ,

Russia, meanwhile, employed domestically produced autonomous platforms including the KUB-BLA and Lancet loitering munitions. The KUB-BLA can deliver a range of payloads and incorporates Artificial Intelligence Visual Identification (AIVI) technology, enhancing real-time recognition and classification of targets, improving the drone's real-time lethality and autonomy.[493] The Lancet, on the other hand, is a

> smart multipurpose weapon, capable of autonomously finding and hitting a target. The weapon system consists of precision strike component, reconnaissance, navigation and communications modules. It creates its own navigation field and does not require ground or sea-based infrastructure and is equipped with several targeting systems: coordinate system, optoelectronic system and combined system.[494]

In addition to these systems, the Iranian semi-autonomous designed loitering munitions Shahed-136 — rebranded as

---

AVINC, *Switchblade 600*, accessible at: https://www.avinc.com/lms/switchblade-600; T. Copp, *Kyiv Asked for a New Kamikaze Drone to Fight Russia. The Air Force Delivered Phoenix Ghost*, Science & Tech, Defense One, 2022, accessible at: https://www.defenseone.com/technology/2022/04/kyiv-asked-new-kamikaze-drone-fight-russia-air-force-delivered-phoenix-ghost/365945/.

[493] Automated Decision Research, op. cit.; Army Technology, *Zala KYB Strike Drone, Russia*, 2023, accessible at: https://www.army-technology.com/projects/zala-kyb-strike-drone-russia/ ; WIRED, *Russia's Killer Drone in Ukraine Raises Fears About AI in Warfare*, 2022, accessible at: https://www.wired.com/story/ai-drones-russia-ukraine/.

[494] Automated Decision Research, op. cit.

Geran-2 under Russian license — capable of carrying a high-explosive warhead, and of conducting a kamikaze-style attack on ground targets, were used by Russia in several attacks.[495] These systems are pre-programmed to fly autonomously, without requiring a human pilot to control them remotely, and can either fly pre-programmed missions or conduct real-time surveillance and reconnaissance, using its onboard sensors to navigate and identify targets.[496]

Importantly, the Shahed-136 (Geran 2) have been reported to attack civilian areas and targeting Ukraine's critical energy infrastructure all over the country.[497] Saba Sotoudehfar notes that according to the United Nations, during October and November of 2022, 92 drone attacks were carried out on Ukrainian energy infrastructure, 77 civilians killed, and severe injuries were caused to 272 non-combatants.[498] As a result, millions of Ukrainians were left without access to electricity, water, heating, and other vital services.[499] The researcher further observes that "the number of casualties among both civilians

[495] S. Sotoudehfar, op. cit., p. 157.
[496] Ibidem.
[497] Ibid., p. 145, see pp. 155-156 for concrete examples of attacks on civilian infrastructure, including power stations, a dam and a hospitals and pp. 159-160 for concrete examples of violations of the principle of proportionality.
[498] Ibidem.
[499] Ibidem.

and combatants is considerably high, revealing that not only are combatants being targeted by these systems, but also, in some cases, civilians and civilian infrastructure, causing harm in violation of IHL principles."[500] This led President Zelensky to accuse Iran of being "complicit in war crimes by supplying these drones."[501]

Indeed, the use of loitering munitions and AI-enhanced weapon systems in densely populated areas has resulted in significant civilian casualties and infrastructural damage — acts that may amount to war crimes. However, these challenges are not unique to Ukraine. This trend is notably evident in the Gaza armed conflict, where, in addition to loitering munitions, AI-supported systems such as *Lavender*, *Gospel*, and *Where is Daddy?* were deployed for the identification, classification, and prioritization of targets using algorithmic processes. These examples signal a global shift toward the normalization of AI-supported targeting systems and weapons, emphasizing the growing legal and ethical challenges posed by increasingly autonomous weapons in armed conflict — particularly in environments where real-time distinction between combatants and civilians is complex or *unreliable*.

[500] Ibid., p. 146.
[501] Ibid., p. 154.

4. THE ARMED CONFLICT IN GAZA (2023-ONGOING)

The roots of the Israeli-Palestinian conflict stretch back over a century, emerging before the collapse of the Ottoman Empire and with the rise of the Zionist movement. It took on a new dimension in 1948, with the establishment of Israel as a state. This event triggered the first Arab-Israeli war and led to the mass displacement of about 750,000 Palestinians — referred to as *Al Nakba* (the catastrophe).[502] Another significant turning point came in 1967, when Israel occupied the West Bank, East Jerusalem, Gaza Strip, Sinai Peninsula, and the Golan Heights following the Six-Day War, initiating a prolonged military occupation that remains central in the ongoing conflict.[503]

In the years that followed, the Palestinian territories experienced prolonged cycles of violence[504], the expansion of

[502] United Nations | The Question of Palestine, *History of the question of Palestine*, n.d., accessible at: https://www.un.org/unispal/history/; BBC, *Israel and the Palestinians: History of the conflict explained*, 2025, accessible at: https://www.bbc.com/news/newsbeat-44124396 ; Council on Foreign Relations, *Israeli-Palestinian Conflict Timeline*, 2024, accessible at: https://education.cfr.org/learn/timeline/israeli-palestinian-conflict-timeline.

[503] United Nations | The Question of Palestine, *History of the question of Palestine*, op. cit.

[504] For example, see United Nations Office for the Coordination of Humanitarian Affairs (OCHA) – occupied Palestinian territory, *The Humanitarian Monitor: OPT (October-November 2012) – OCHA report*,

Israeli settlements deemed illegal under international law,[505] and a systemic blockade — now in its second decade — particularly over the Gaza Strip.[506] In particular, in May 2021, tensions escalated in East Jerusalem, notably in the Sheikh Jarrah neighborhood, where the eviction of Palestinian families sparked widespread protests.[507] The situation intensified when Israeli forces clashed with worshipers at Al-Aqsa Mosque in the following days. In response, Hamas launched rockets into Israel, the latter responded with extensive airstrikes on Gaza.[508] The 11-day military confrontation between Israel and Hamas

2012, accessible at: https://www.un.org/unispal/document/auto-insert-201184/

[505] International Court of Justice (ICJ), *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 9 Jul 2004 and International Court of Justice (ICJ), *Legal Consequences of Israel's Policies and Practices in the Occupied Palestinian Territory, including East Jerusalem*, Advisory Opinion, 19 Jul 2024.

[506] Amnesty International, *Israel's Occupation: 50 Years of Dispossession*, 2017, accessible at: https://www.amnesty.org/en/latest/campaigns/2017/06/israel-occupation-50-years-of-dispossession/.

[507] United Nations Office for the Coordination of Humanitarian Affairs (OCHA), *Escalation in the West Bank of the Gaza Strip and Israel Flash Update #1 as of 17,00, 11 May 2021*, accessible at: https://www.ochaopt.org/content/escalation-west-bank-gaza-strip-and-israel-flash-update-1-1700-11-may-2021 and United Nations Office for the Coordination of Humanitarian Affairs (OCHA), *West Bank: Escalation of Violence 13 April – 21 May 2021*, accessible at: https://www.ochaopt.org/content/west-bank-escalation-violence-13-april-21-may-2021.

[508] Ibidem.

resulted in the death of at least 256 Palestinians, including 66 children and 40 women, and 13 Israelis, including two children and six women, marking — at the time — one of the deadliest escalations since 2014.[509]

In the wake of that escalation, and just over two years later, on October 7, 2023, Hamas launched an unprecedented cross-border assault on Israel, killing 1,200 people — predominantly civilians — and taking 255 hostages into Gaza.[510] During the attacks, Hamas relied heavily on improvised weaponry and extensively deployed unmanned aerial systems (UAS), particularly small, tactical drones.[511] These drones "constituted the first wave of attacks to eliminate Israeli observation towers, cameras, and communications."[512] Their use effectively

[509] United Nations Office for the Coordination of Humanitarian Affairs (OCHA), *Protection of Civilians Report* | 24-31 May 2021, accessible at: https://www.ochaopt.org/poc/24-31-may-2021.

[510] Israeli Ministry of Foreign Affairs, *Swrods of Iron: Hostages and Missing Persons Report,* 2023, updated 12 May 2025, accessible at: https://www.gov.il/en/pages/hostages-and-missing-persons-report; Reuters, *Israel revises Hamas attack death toll to 'around 1200'*, 10 Nov 2023, accessible at: https://www.reuters.com/world/middle-east/israel-revises-death-toll-oct-7-hamas-attack-around-1200-2023-11-10/.

[511] L. Dogson | Business Insider, *Hamas used drone bombs to launch its war on Israel from Gaza, and took out hi-tech observation towers, videos show*, 8 Oct 2023, accessible at: https://www.businessinsider.com/video-hamas-used-drone-bombs-to-launch-war-with-israel-2023-10?r=US&IR=T.

[512] K. Chávez and O. Swed, *How Hamas innovated with drones to operate like an army*, Bulletin of the Atomic Scientists, 2023, accessible at:

disrupted Israel's early-warning systems and neutralized several automated defense installations, helping facilitate the subsequent ground incursions.[513]

In the hours and days that followed, Hamas employed a range of drone tactics, including the dropping of munitions on tanks and the coordination of drone swarms to target naval vessels and energy infrastructure — mirroring military-grade operations and state-like combat strategies.[514] In addition to commercially available quadcopters, Hamas relied on a loitering munition known as the *Zouari*.[515] The Zouari drone functioned as a "DIY [do it yourself] suicide drone",[516] intended to dive onto targets with an explosive payload. While its exact technical specifications remain unclear, available analyses

https://thebulletin.org/2023/11/how-hamas-innovated-with-drones-to-operate-like-an-army/.

[513] M. Jankowicz | Business Insider, *How Hamas likely used rudimentary drones to 'blind and deafen' Israel's border and pave the way for its onslaught,* 10 Oct 2023, accessible at: https://www.businessinsider.com/hamas-drones-take-out-comms-towers-ambush-israel-2023-10.

[514] K. Chávez and O. Swed, op. cit., accessible at: https://thebulletin.org/2023/11/how-hamas-innovated-with-drones-to-operate-like-an-army/.

[515] Ibidem.

[516] Ibidem.

suggest it lacks the ability to independently select or engage targets in real-time.[517]

From a legal standpoint, Hamas's use of drones does not inherently violate IHL where the targets were clearly military in nature, such as tanks, surveillance towers, or troop formations. However, the use of indiscriminate rockets, the targeting of civilian areas, and the deliberate abduction and hostage taking of civilians constitute grave breaches of IHL and form the core of potential war crimes for which Hamas commanders and political leaders may bear responsibility in this conflict.[518]

These breaches — committed directly by human militants and operatives rather than by autonomous systems — not only underscore the enduring importance of human accountability in the conduct of hostilities, but also raise significant concerns

[517] P. Satam , *Hamas reveals "Zouari" kamikaze drone that can potentially rain hell on israel During Gaza Ops*, The EurAsian Times, 12 Oct 2023, accessible at: https://www.eurasiantimes.com/hamas-reveals-zouari-kamikaze-drone-that-can-potentially-rain/; the reporter notes: "whether the Zouaris are remotely controlled, fully or semi-autonomous is unclear. [...] It is unlikely that the UAV has advanced features that can abort an attack or bring it back to the operator". Such advanced features will "require more incredible industrial infrastructure and access to the advanced machines, which Hamas does not [have]".

[518] International Criminal Court (ICC), *Statement of ICC Prosecutor Karim A.A. Khan KC: Applications for arrest warrants in the situation of the State of Palestine*, Office of the Prosecutor, 20 May 2024, accessible at: https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-applications-arrest-warrants-situation-state.

regarding the growing capacity of non-state actors to acquire and operate increasingly sophisticated weapon systems. The implications of this trend are alarming: when non-state actors possess access to truly autonomous weapon systems, capable of selecting and engaging targets independently, the scale and unpredictability of damage would likely be significantly greater. This concern, while still speculative in the case of non-state actors, becomes all the more tangible when one turns to the conduct of technologically advanced states that already deploy algorithmic and AI-enabled targeting systems in ongoing conflicts.

The Israeli military campaign in Gaza provides a particularly stark illustration — not of a hypothetical risk or a future scenario to be feared, but of a present-day reality in which "supervised" autonomy, reflected in predictive targeting and extensive use of AI-enabled loitering munitions, has effectively reshaped the conduct of hostilities. It is important, in this regard, to note that, these tools were not entirely new — Israel has, according to investigative reports, for years treated Gaza as "a testing ground for new technologies and weaponry"[519] — but since 2023, their deployment reached new levels and scales of autonomy.

[519] M. Fatafta and D. Leufer, *Artificial Genocidal Intelligence: how Israel is automating human rights abuses and war crimes*, Access Now, 9 May 2024, accessible at: https://www.accessnow.org/publication/artificial-

Two broad categories of Israeli systems stand out: loitering munitions and armed drones, and AI-supported targeting systems. As previously mentioned, Israel's defense industry has long been a pioneer in loitering munitions. In addition to its most well-known loitering munition the Harop and its successors, other systems were employed in Gaza including the *Rotem L*, the *Green Dragon*, and re-purposed commercial quadcopter drones used to drop munitions or to carry firearms– nicknamed "sniper drones".

The IAI Rotem L[520] — a tactical expendable loitering munition designed specifically for urban warfare — can be carried and operated by a single soldier and deployed in under a minute.[521] It carries a 6.5 kg explosive warhead and can fly quietly for up to 45 minutes while seeking a target.[522] Once a

genocidal-intelligence-israel-gaza/#:~:text=fully%20automated%20"killer%20robots"%20on,driven%20horrors; S. Cohen, Shark Tanks: With Gaza as Testing Ground, Israeli Defense Startups Flourish, HAARETZ, 3 Jan 2024, accessible at: https://www.haaretz.com/israel-news/2024-01-03/ty-article-magazine/.premium/suicide-drones-and-ai-with-gaza-as-testing-ground-israeli-defense-startups-flourish/0000018c-cf39-ddba-abad-cfb9a3ee0000.

[520] TVD.IM, *IAI Rotem L*, n.d., accessible at: https://tvd.im/aviation/1089-iai-rotem-l.html.

[521] Quds News Network | Just International, *Israel Uses Suicide Drones Against Gatherings of Displaced Families*, 22 Apr 2025, accessible at: https://just-international.org/articles/israel-uses-suicide-drones-against-gatherings-of-displaced-families/.

[522] Ibidem.

target is identified and locked on, the Rotem L dives in to crash and detonate.[523] It is equipped with AI-powered guidance that gives it a degree of autonomy in navigating and homing in on targets.[524] Importantly, the Rotem L functions in a human-on-the-loop mode, allowing operators to recall, reroute or abort strikes if needed. In practice, however, observers have noted that this human-on-the-loop control was/is often nominal; the drones were rarely recalled and were deliberately used to target civilian gatherings.[525]

The Green Dragon[526] — a tube-launched, silent loitering munition designed for tactical-level operations — offers real-time ISR combined with immediate strike capability.[527] With a range of up to 40 km and a loitering time of 1.5 hours, the Green Dragon is capable of autonomously navigating toward pre-programmed coordinates or dynamically adjusting its flight path based on ISR data.[528] It is equipped with electro-optical sensors and a 3 kg warhead, and like the Rotem L, operates in a human-

[523] Ibidem.
[524] Ibidem.
[525] Ibidem.
[526] IAI Green Dragon, TVD | Tactical Missiles, accessible at: https://tvd.im/aviation/1081-iai-green-dragon.html.
[527] Ibidem.
[528] Ibidem.

on-the-loop mode, with the possibility of operator intervention before terminal engagement.[529]

In addition to standard military loitering munitions, Israeli forces have also re-purposed commercial quadcopters and off-the-shelf drones for offensive purposes. Though less sophisticated than systems like the Harop or Green Dragon, these modified drones have been reportedly deployed to target civilians and civilian infrastructure, raising serious alarms regarding compliance with IHL principles.[530]

Throughout 2024 and into mid 2025, Israeli military operations in Gaza remained intense. The Israel Defense Forces (IDF) campaign, entailed massive bombardment of Gaza's densely populated urban areas, razing entire neighborhoods and resulting in a cumulative Palestinian death toll exceeding 50,000 persons — the majority of whom are women and children — by March 2025, according to the United Nations

[529] Ibidem.

[530] K. Lonsdorf, *Eyewitnesses in Gaza say Israel is using spiner drones to shoot Palestinians*, NPR, 26 Nov 2024, accessible at: https://www.npr.org/2024/11/26/g-s1-35437/israel-sniper-drones-gaza-eyewitnesses; AlJazeera, *Israel retrofitting DJI commercial drones to bomb and surveil Gaza*, 8 May 2025, accessible at: https://www.aljazeera.com/news/2025/5/8/israel-retrofitting-dji-commercial-drones-to-bomb-and-surveil-gaza; S. Ackerman, *Israel's Armed Quadcopters in Gaza Mark a Dangerous New Era in Drone Warfare*, Zeteo, 29 Apr 2024, accessible at: https://zeteo.com/p/israel-gaza-quadcopter-drone-warfare.

briefings, amounting to approximately 2% of Gaza's population.[531] The strikes also resulted in over 110,000 wounded Gazans and displaced approximately 1.9 million (around 90% of Gaza's population) from their homes.[532]

A direct contributor to this enormous death and destruction toll — and perhaps the most controversial high-tech tools used by Israel in this war — were its AI-driven targeting systems. According to multiple investigative reports, the IDF relied heavily on a suite of algorithms to generate target lists and identify individuals and infrastructure for attack. Chief among these systems were "*The Gospel*" (in Hebrew, Hab'sora), "*Lavender*", and "*Where is Daddy?*"[533]

---

[531] United Nations Office for the Coordination of Humanitarian Affairs (OCHA), *Humanitarian Situation Update #275 | Gaza Strip, 27 Mar 2025*, accessible at: https://www.un.org/unispal/document/ocha-humanitarian-situation-update-275-gaza-strip/; The update notes that "[s]ince 7 October 2023 and as of 25 March 2025, the MoH in Gaza reported that at least 50,144 Palestinians have been killed and 113,704 Palestinians injured".

[532] Ibidem.; see The Guardian, *A visual guide to the destruction of Gaza*, 18 Jan 2025, accessible at: https://www.theguardian.com/world/2025/jan/18/a-visual-guide-to-the-destruction-of-gaza.

[533] Y. Abraham, '*Lavender': The AI machine directing Israel's bombing spree in Gaza*, +972 Magazine, Investigative Report, 3 Apr 2024, accessible at: https://www.972mag.com/lavender-ai-israeli-army-gaza/ ; Y. Abraham, *'A mass assassination factory': Inside Israel's calculated bombing of Gaza*, Investigative Report, 30 Nov 2023, accessible at: https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/.

The *Gospel* is described as an automated target generation system focused on infrastructure targets.[534] It ingests intelligence data (satellite imagery, signals intercepts, databases of buildings, etc.) and produces recommendations for which structures to strike — presumably those assessed to be Hamas command centers, weapons depots, and/or tunnel entrances.[535] By using pattern recognition and predictive algorithms[536], Gospel can scan the vast urban terrain of Gaza for signs of militant activity. IDF commanders can then select from this algorithm-curated list of sites for bombing.[537]

---

[534] M. Fatafta and D. Leufer, *Artificial Genocidal Intelligence: how Israel is automating human rights abuses and war crimes,* op. cit.

[535] Y. Abraham, *'A mass assassination factory': Inside Israel's calculated bombing of Gaza,* op. cit.; see also: The Washington Post, *Israel built an 'AI factory' for war. It unleashed it in Gaza*, 29 Dec 2024, accessible at: https://www.washingtonpost.com/technology/2024/12/29/ai-israel-war-gaza-idf/.

[536] In 2020, a coalition of expert researchers and practioners across various fields addressed an open letter to Springer condemning predictive criminality and how such systems can reinforce bias. These concerns are equally relevant in the context of armed conflict, where predictive targeting may lead to unlawful strikes, undermining IHL principle of distinction and precaution. See: Coalition for Critical Technology, *Abolish the Tech-to-Prison Pipeline*, 23 Jun 2020, accessible at : https://medium.com/@CoalitionForCriticalTechnology/abolish-the-techtoprisonpipeline-9b5b14366b16.

[537] Y. Abraham, *'A mass assassination factory': Inside Israel's calculated bombing of Gaza,* op. cit.; The investigative article cites one source who worked in the new Targets Administrative Division: "[w]e prepare the targets automatically and work accroding to a checklist". The source continues: "[i]t really is like a factory. We work quickly and there is no

Lavender is a parallel system, but focused on individual human targets.[538] Essentially, it analyzes communications, social media, informant tips, and other surveillance to identify persons likely affiliated with Hamas or Palestinian Islamic Jihad (PIJ).[539] It tracks patterns of movement and behavior that match profiles of known militants. In the Gaza war, Lavender automatically compiled "kill lists" of people it deemed militant operatives, along with their suspected locations.[540] *Where is Daddy?* is an AI tool that tracks these targeted individuals and alerts Israeli forces when they are at home with their families.[541]

In other words, once Lavender has identified a person and their residence, Where is Daddy? monitors for the presence of that person at the home and effectively cues a strike at that moment. The nickname "Where is Daddy?" reflects that the system's purpose is to find a militant in the one place he is virtually guaranteed to eventually return — his family home — even if that means his family will likely be there too.[542]

---

time to delve deep into the target. The view is that we are jugded accroding to how many targets we manage to generate".

[538] M. Fatafta and D. Leufer, *Artificial Genocidal Intelligence: how Israel is automating human rights abuses and war crimes,* op. cit.

[539] Y. Abraham, '*Lavender': The AI machine directing Israel's bombing spree in Gaza*, op. cit.

[540] Ibidem.

[541] M. Fatafta and D. Leufer, *Artificial Genocidal Intelligence: how Israel is automating human rights abuses and war crimes,* op. cit.

[542] Ibidem.

What is most problematic about these systems, is not only that they reduce human lives to data points, but also that the data sets they were trained on were flawed, leading to frequent misidentification of civilians as militants.[543] For instance, Lavender drew on lists of employees of Hamas civil administration in Gaza (non-combatants), their relatives, and "even individuals who merely had the same name as Hamas operatives"[544] and flagged them all as targets. According to Israeli military sources, the system's error rate in identifying a person's affiliation was around 10%[545] — meaning one in ten people it designated as Hamas/PIJ militant was actually a civilian with no combatant activity or links to armed groups.

Despite awareness of this error rate, the IDF obtained "sweeping approval to automatically adopt [Lavender's] kill list

[543] Y. Abraham, '*Lavender': The AI machine directing Israel's bombing spree in Gaza*, op. cit. "One source who worked with the military data science team that trained Lavender said that data collected from employees of the Hamas-run Internal Security Ministry, whom he does not consider to be militants, was also fed into the machine. "I was bothered by the fact that when Lavender was trained, they used the term 'Hamas operative' loosely, and included people who were civil defense workers in the training dataset," he said".

[544] M. Fatafta and D. Leufer, *Artificial Genocidal Intelligence: how Israel is automating human rights abuses and war crimes,* op. cit.; see also Y. Abraham, '*Lavender': The AI machine directing Israel's bombing spree in Gaza*, op. cit.

[545] Y. Abraham, '*Lavender': The AI machine directing Israel's bombing spree in Gaza*, op. cit.

'as if it were a human decision.'"[546] In practice, this meant an algorithm's output was treated with the same authority as a carefully vetted intelligence finding by a human. Statements from head of the Israeli Military's Artificial Intelligence Center (Unit 8200-IDF) and reports from sources including the Israeli *+972 Magazine* indicate that these AI systems generated thousands of targets in a matter of days — a task that would previously take intelligence officers several weeks.[547] Additionally, human control was limited to a cursory gender check, that according to interviewed Lavender operators, took about "20 seconds" — only to confirm that the target is a male.[548]

Even more problematic was the so-called tolerated collateral damage degree. According to the investigation led by *+972*

---

[546] M. Fatafta and D. Leufer, *Artificial Genocidal Intelligence: how Israel is automating human rights abuses and war crimes,* op. cit.

[547] Israel Defense, *לראשונה נחשף: כך פועלת מערכת הבינה המלאכותית של צה"ל במבצעי סיכול ממוקד* [For the first revealed: How the IDF's artificial intelligence system operates in targeted operations], Nov 10 2022, available in Hebrew at: https://www.israeldefense.co.il/node/57256#google_vignette (translated into English using ChatGPT-4o) "One of the most important tools we have built and currently operate is a system that can identify 'dangerous' individuals based on input from a list of people already flagged and fed into the system. This process is carried out by the system in seconds—something that previously would have taken hundreds of investigators several weeks to complete."; Y. Abraham, '*Lavender': The AI machine directing Israel's bombing spree in Gaza*, op. cit.

[548] Y. Abraham, *'Lavender'* [...], op. cit.

Magazine, some IDF officers and system operators revealed that, during the initial phase of the war, the Israeli military approved fixed collateral damage degrees per strike, allowing the killing of up to 15 or even 20 civilians alongside each junior Hamas operative targeted by Lavender.[549] These thresholds were applied indiscriminately, regardless of the militant's rank, military value, or precise location, and without conducting a case-by-case proportionality assessment as required under IHL.

This pattern was extended and intensified in strikes targeting Hamas commanders. For instance, the same investigation reported that, in the assassination operation of Ayman Nofal, the commander of Hamas' Central Gaza Brigade, the army authorized "the killing of approximately 300 civilians, destroying several buildings in airstrikes on Al-Bureij refugee camp [...] based on an imprecise pinpointing of Nofal".[550]

From a legal perspective, the scale, tempo, and method of these AI-facilitated operations significantly stretch the normative framework of IHL to its limits. While the IDF claims compliance with the core principles of distinction, proportionality, and precaution,[551] the sheer volume of strikes

[549] Ibidem.
[550] Ibidem.
[551] The Guardian, *Israel Defence Forces' response to claims about the use of 'Lavender' AI database in Gaza*, Apr 3 2024, accessible at:

and the evident civilian toll raise serious doubts.[552] UN reports have questioned whether indiscriminate or disproportionate attacks have occurred, especially given the use of explosive weapons with wide-area effects (e.g., MK83, GBU-31, GBU-32, and GBU-39 bombs) in densely populated areas without prior warning.[553] The targeting of civilian infrastructure, such as hospitals, markets, and refugee camps, has raised concerns of potential war crimes for which Israeli commanders and political leaders may bear responsibility in this conflict,[554] and the

https://www.theguardian.com/world/2024/apr/03/israel-defence-forces-response-to-claims-about-use-of-lavender-ai-database-in-gaza.

[552] United Nations Office of the High Commissioner for Human Rights (OHCHR), Pattern of Israeli attacks on Gaza hospitals raises grave converns – report, Dec. 31 2024, accessible at: https://www.ohchr.org/en/press-releases/2024/12/pattern-israeli-attacks-gaza-hospitals-raises-grave-concerns-report.

[553] United Nations Office of the High Commissioner for Human Rights (OHCHR), *Thematic Report: Attacks on hospitals during the escalation of hostilities in Gaza (7 October 2023-30 June 2024)*, Dec 31 2024, p. 19-20, accessible at: https://www.ohchr.org/sites/default/files/documents/countries/opt/20241231-attacks-hospitals-gaza-en.pdf and United Nations Office of the High Commissioner for Human Rights (OHCHR), *Thematic Report: Indiscriminate and disproportionate attacks during the conflict in Gaza (October – December 2023)*, Jun 19 2024, p. 4 and p. 10-16, accessible at: https://www.ohchr.org/sites/default/files/documents/countries/opt/20240619-ohchr-thematic-report-indiscrim-disprop-attacks-gaza-oct-dec2023.pdf.

[554] International Criminal Court (ICC), *Statement of ICC Prosecutor Karim A.A. Khan KC: Applications for arrest warrants in the situation of the State of Palestine*, 2024, op. cit.

International Court of Justice (ICJ) has affirmed that plausible genocide claims exist under the Genocide Convention.[555]

Unlike in other contexts, where AWS and AI have been used primarily to gain battlefield advantage, the war in Gaza demonstrates how algorithmically generated targeting lists — when combined with expansive definitions of combatants and relaxed operational constraints — can result in the systematic automation of mass violence. The claim advanced by proponents of AWS — that these systems, due to their precision, lack of emotional bias, and ability to make rapid decisions based on mathematical calculations and structured data, are more compliant with IHL and promote more humane warfare — is clearly challenged by empirical realities, particularly in the armed conflicts in Ukraine and Gaza.

In other words, the rising deployment of AI-enabled offensive weapon systems — especially loitering munitions — when paired with algorithmic targeting, marks a dangerous turning point in the evolution of warfare. This remains the case despite the fact that none of these systems concretely fit the

[555] International Court of Justice (ICJ), *Application of the Convention on the Prevention and Punishment of the Crime of Genocide in the Gaza Strip (South Africa v. Israel),* Order on the Request for the Indication of Provisional Measures, Jan 26 2024, §54.

narrow definition of AWS, as they cannot **yet** complete the full targeting and engagement cycle independently of human input.

This reality, however, prompts two observations. First, full autonomy may not require a single, all-in-one, 'autonomous weapon system'; it may instead emerge through the integration of multiple automated systems and components — raising the question: is the real issue the notion of an autonomous weapon, or the broader process of automation of the tactical and operational phases of warfare? Second, the mere presence of human involvement does not ensure meaningful control over the targeting process. In practice, human roles can become purely formalistic or symbolic, especially when decisions are heavily influenced — if not outright determined — by AI-generated recommendations or kill lists.

These developments suggest that the risks associated with autonomy in warfare lie not only in machines acting autonomously, but more generally in the dilution of human judgment over decisions to kill or destroy within increasingly automated chains of command. This shift not only signals the emergence of a new form of warfare, but also reflects a profound redefinition of how lethal decisions are made — and by whom — challenging the long-standing, human-centered paradigm that has underpinned the laws and ethics of war for centuries.

CONCLUSIONS AND RECOMMENDATIONS

More than 150 years after the adoption of the St. Petersburg Declaration, the core concern it articulated — that the progress of civilization should alleviate, not exacerbate, the calamities of war — remains profoundly relevant.

This analysis began by confronting the absence of a consensual definition of AWS — a gap that is neither insignificant nor coincidental. As this research has demonstrated, definitional fragmentation has direct consequences: it influences how these systems are legally qualified, how their use is regulated under international law, and how standards for human control, accountability, and IHL compliance are determined.

While none of the systems examined in this study meets the strict definition of a fully autonomous weapon system — that is, one capable of completing the entire targeting cycle without human intervention, and endowed with the technical ability to make cognitively and morally complex decisions — what emerges from practice is equally alarming. The combined functionality of increasingly autonomous systems, when integrated into military operations, creates a cumulative effect that closely approximates full autonomy. This trajectory does not entirely eliminate human involvement — it dilutes it,

rendering it more procedural than meaningful. This allows for highly automated targeting chains without ever breaching the narrow technical threshold of "full autonomy."

More troubling, the evolution of AWS makes a shift in paradigm: from machines designed to replicate or support human reasoning, to human actors being compelled to validate or match the outputs of the machine without further reasoning. The testimonies cited in investigative reports by +972 Magazine corroborate this shift.[556] Where algorithms identify hundreds of targets in a single operation, human operators are pressured to escalate output. Processes that previously required human deliberation and time — often measured in weeks or months — are now compressed into hours or days by software and data-driven models.

Compounding this is growing evidence that human operators tend to treat automated suggestions with the same, if not greater, authority than their own judgment.[557] This general

[556] Y. Abraham, '*Lavender': The AI machine directing Israel's bombing spree in Gaza*, accessible at: https://www.972mag.com/lavender-ai-israeli-army-gaza/ ; Y. Abraham, *'A mass assassination factory': Inside Israel's calculated bombing of Gaza*, accessible at: https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/.

[557] M. L. Cummings, *Automation Bias in Intelligent Time Critical Decision Support Systems*, in AIAA 1st Intelligent Systems Technical Conference, 20-22 Sep 2004, AIAA 2004-6313, accessible at: https://arc.aiaa.org/doi/10.2514/6.2004-6313.

trend, known as automation bias, extends to human decision-makers who may defer to algorithmic outputs even when these are flawed or contextually inadequate.[558] The consequence of such bias is the gradual erosion of human cognition and agency in battlefields — a dangerous outcome, especially considering its lethal implications.

The reference at the beginning of Chapter 2 to the realist, managerial, and idealist approaches to war and peace was not without reason. It was meant to serve as a reminder of a historical trajectory that seems increasingly marginalized.

War is as old as human civilization. Against the backdrop of a cumulative inheritance of brutal conflicts, humans created the laws of war, and countered them with the laws of humanity. When the brutality threshold went out of control in the two World Wars, and harms "spilled" from the sphere of military to the sphere of the civilian, the global community collectively agreed to prohibit the threat or use of force in international relations. This prohibition — on the legal level — was continuously reinforced, sometimes in symbolic ways, such as renaming "the law of war" into "the law of armed conflict," and later "international humanitarian law," and sometimes in more

[558] V. Boulanin, N. Davison,, M. Verbruggen, and N. Goussac, *Limits on Autonomy in Weapon Systems: Identifying Practical Elements of Human Control*, SIPRI and ICRC, 2020, p. 19.

substantive ways, such as through disarmament and arms control treaties, weapons review and the institutionalization of peaceful dispute settlement mechanisms. All these collective efforts were undertaken to "save succeeding generations from the scourage of war" and preserve "the dignity and worth of the human person," as enshrined in the Preamble of the UN Charter.

One can argue that the ultimate objective is not to render war "more humane," but to avoid it altogether. Even the premise of a more humane war is questionable, because empirical evidence show that emerging technologies accelerated the decision to use force and increased the toll of death and destruction — sometimes exceeding 50,000 people and 90% of civilian cities and infrastructure — clearly challenging this assumption.

It is in this sense that the joint warning issued by the UN Secretary-General and the President of the ICRC — that delegating targeting decisions to machines risks lowering the threshold for the use of force and escalating conflicts, thereby posing a serious threat to international peace and security — must be taken seriously.[559] This is also why discussing AWS

[559] United Nations Secretary-General and President of the International Committee of the Red Cross, *Note to Correspondents: Joint call by the United Nations Secretary-General and the President of the International Committee of the Red Cross for States to establish new prohibitions and*

within the framework of the UN carries symbolic weight. It reflects a shared understanding — at least in principle — that the issue transcend national borders and military doctrines and is of a universal concern.

While states widely recognize the CCW is as the primary venue for the discussion, and while significant diplomatic efforts have been made over the past decade, the legal outcome remains absent. This absence is — at least — formally justified by the consensus-based decision-making process required to grant a mandate to start negotiating an international treaty on AWS. This procedural obstacle renders the adoption of a legal instrument under the CCW somewhat unlikely as long as a handful of militarily advanced states oppose binding regulation.

In an optimistic shift, the UN General Assembly adopted two successive resolutions on LAWS – A/RES/78/241 in 2023 and its updated version in 2024 – each with overwhelming support: 152 and then 161 voting in favor.[560] These resolutions reaffirmed the urgent need for international regulation and called for the negotiation of a legally binding instrument to

restrictions on Autonomous Weapon Systems, 5 Oct. 2023, accessible at: https://www.un.org/sg/en/content/sg/note-correspondents/2023-10-05/note-correspondents-joint-call-the-united-nations-secretary-general-and-the-president-of-the-international-committee-of-the-red-cross-for-states-establish-new

[560] United Nations General Assembly, A/RES/78/241 and A/RES/79/239.

ensure meaningful human control over the use of force. Although not legally binding, they reflect growing global consensus that the issue can no longer be stalled and an international action is needed — further confirming that AWS are a global concern that threatens all states. This shift came in response to the UN Secretary-General's *New Agenda for Peace*, which explicitly urged states to conclude an international treaty on AWS by 2026.[561]

Whether such a treaty will be proposed — and more importantly, whether it will be accepted by the states that develop and deploy these systems — remains uncertain. But what remains certain, however, is that any normative framework addressing AWS — whether under the scope of IHL, through the CCW, a distinct treaty, or through soft law and non-binding responsible practices — must account for the definitional, legal, and operational challenge these systems pose.

It is on this basis that the following recommendations are proposed:

[561] A. Guterres, *A New Agenda for Peace*, United Nations Secretary-General, July 2023, p. 27, accessible at: https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-new-agenda-for-peace-en.pdf.

1. **Overcome the lack of consensus over the definition of AWS.**

An inclusive working definition of AWS that acknowledges degrees of autonomy and accounts for distributed systems is urgently needed. This definition should not be overly anchored in one single approach — be it human-centric, task-centric, or technology-centric — but should instead reflect a balanced integration of all three. The nature of the task performed, the spectrums of human–machine interaction, and the sophistication of the software and decision-making architecture are all essential elements to account for. They must be considered jointly to distinguish between fully autonomous weapon systems and highly automated systems, and to clarify the acceptable thresholds of autonomy in relation to the roles and responsibilities of human operators and commanders. Such definitional clarity is a necessary precondition for any future normative framework on AWS.

2. **Adopt a two-tiered approach to classification and regulation.**

An increasing number of States are now advocating a two-tiered approach that distinguishes between fully autonomous weapon systems and those that display various degrees of autonomy in their functioning. This distinction is pertinent, as it

allows for tailored regulatory responses: systems operating with full autonomy — capable of independently selecting and engaging targets without meaningful human control — should be subject to stricter legal constraints or prohibitions. Conversely, systems with partial or supervised autonomy may be regulated under more nuanced frameworks, provided they incorporate robust safeguards for compliance with IHL and ensure meaningful human control.

3. **Prioritize meaningful human control as a legal requirement.**

The operationalization of the concept of meaningful human control helps avoid regulatory loopholes and nominal forms of human intervention. Human control should not be reduced to token oversight or *post hoc* review; it must be substantive, continuous, and context-sensitive — particularly during the critical phases of target selection and engagement. Future legal instruments should incorporate minimum standards for such control, firmly grounded in IHL obligations.

Moreover, regulatory frameworks should address not only fully autonomous systems but also partially autonomous architectures that, in aggregate, may generate comparable operational and legal risks. The distribution of autonomy across multiple systems — for instance, combining independent

targeting algorithms with loitering munitions (suicide drones), autonomous armed UAVs, or unmanned ground vehicles — may create the illusion of human control, especially since many of these systems still formally operate with a human *in* or *on* the loop. In reality, however, technological advancements are progressively sidelining human cognition and agency. Without clear standards, such fragmentation can undermine compliance with IHL principles, and complicate post-incident legal accountability in cases of IHL violations. Ensuring meaningful human control, therefore, must not be treated as a merely ethical imperative, but as a crucial legal safeguard — one that ensures weapons remain tools used by combatants, subject to weapons law, and that human agents deploying them remain legally responsible for their use, in conformity with targeting law.

4. **Promote transparent legal reviews in line with Article 36 of Additional Protocol** I.

States should be strongly encouraged to conduct thorough legal weapons reviews in accordance with Article 36 of AP I. These reviews should assess not only the weapon's compliance with IHL but also the adequacy of human control mechanisms and the broader operational context in which the system is deployed. Where appropriate, states should consider sharing findings to support transparency and foster collective learning.

To ensure the quality and consistency of such reviews, cross-disciplinary collaboration is essential. Legal, technical, military experts, and ethicists must be actively involved to ensure that weapons reviews remain meaningful, informed, and adequately responsive to the challenges posed by AWS.

5. Regulate state-level proliferation of AWS.

To prevent the unchecked spread of AWS, states should consider addressing not only the end products but also the transfer of critical components — including dual-use software and algorithms, sensor suites, and integrated platforms that enable autonomy. Proliferation risks are particularly aggravated when such systems or components are exported without adequate legal reviews or safeguards to ensure compliance with IHL. Existing arms control regimes should be adapted to incorporate AWS specific criteria and clear use restrictions. This is essential to avoid fragmented standards and legal loopholes that facilitate irresponsible transfers and misuse.

6. Prevent acquisition and misuse of AWS by non-state actors.

Given the increasing availability of commercial components and open-source AI tools, regulatory frameworks must include safeguards to prevent the diversion, theft, or reverse-

engineering of autonomous systems. This includes stricter controls over the development, storage, and access to autonomy-enabling technologies, as well as strengthened international cooperation in intelligence-sharing and enforcement mechanisms. These measures are essential to prevent the potential acquisition or repurposing of AWS by non-state actors — a scenario that further threatens international peace and security.

7. **Promote independent monitoring and empirical transparency of AWS use**.

The opacity surrounding the development, testing, and deployment of autonomous weapon systems remains a significant barrier to effective regulation. Independent monitoring — including investigative journalism, NGOs and Think Tanks reporting, and academic research — plays a critical role in documenting empirical patterns of use, verifying compliance with international law, and identifying emerging risks and loopholes.

States should be encouraged to enhance transparency by cooperating with independent observers and supporting the establishment of international monitoring mechanisms. Such efforts will not only strengthen accountability but also

contribute to a more evidence-based and informed regulatory framework.

The recommendations outlined above reflect the urgent need for a multidimensional framework to address AWS — one that is fundamentally grounded in global cooperation and a collective will to ensure that the future of armed conflict is not shaped by what machines can do, but by what humanity consciously chooses not to delegate to them ...

***

BIBLIOGRAPHY

A. LEGAL INSTRUMENTS AND OFFICIAL DOCUMENTS

➢ TREATIES, CONVENTIONS, AND DECLARATIONS

- Charter of the United Nations, 26 June 1945.
- Convention on Cluster Munitions, 30 May 2008.
- 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, 10 October 1980.
- Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, 10 April 1972.
- Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, 13 January 1993.
- Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction, 18 September 1997.
- Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight (St. Petersburg Declaration), 29 November / 11 December 1868.
- Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War, 12 August 1949.
- Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.
- Protocol on Blinding Laser Weapons (Protocol IV to the 1980 Convention), 13 October 1995.
- Protocol on Prohibitions or Restrictions on the Use of Incendiary Weapons (Protocol III to the 1980 Convention), 10 October 1980

- Regulations concerning the Laws and Customs of War on Land, annexed to the Hague Convention (IV) respecting the Laws and Customs of War on Land, 18 October 1907.
- Rome Statute of the International Criminal Court, 17 July 1998.

➢ UNITED NATIONS RESOLUTIONS, REPORTS AND OFFICIAL DOCUMENTS

- Group of Governmental Experts on Emerging Technologies in the Area of Autonomous Weapons Systems, *Report of the 2018 session*, CCW/GGE.1/2018/3, 2018.
- Group of Governmental Experts on Emerging Technologies in the Area of Autonomous Weapons Systems, *Non-exhaustive compilation of definitions and characterizations*, CCW/GGE.1/2023/CRP.1, 2023, accessible at: https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_CRP.1_0.pdf
- Group of Governmental Experts on Emerging Technologies in the Area of Autonomous Weapons Systems, *Chairperson's Summary*, CCW/GGE.1/2020/WP.7, 2021.
- Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, *Compilation of Replies Received to the Chair's Guiding Questions*, CCW/GGE.1/2024/CRP.1, 2024, accessible at : https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2024)/CCW_GGE1_2024_CRP1.pdf.
- Guterres, A., *Lethal Autonomous Weapons Systems : Report of the Secretary-General*, UN Secretary-General, A/79/88, 2024, accessible at: https://docs-library.unoda.org/General_Assembly_First_Committee_-Seventy-Ninth_session_(2024)/A-79-88-LAWS.pdf.

- Heyns, C., *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions*, UN Human Rights Council, A/HRC/23/47, 2013.
- UN Security Council, *Final report of the Panel of Experts on Libya established pursuant to Security Council resolution 1973*, S/2021/229, 2021, accessible at: https://digitallibrary.un.org/record/3905159?v=pdf.
- United Nations General Assembly, *Resolution 78/241: Lethal Autonomous Weapons Systems,* A/RES/78/241, adopted on 22 December 2023, accessible at: https://docs.un.org/en/A/RES/78/241.
- United Nations General Assembly, *Resolution 79/239: Artificial intelligence in the military domain and its implications for international peace and security*, A/RES/79/239, adopted on 24 December 2024, accessible at: https://unidir.org/wp-content/uploads/2025/03/UN_General_Assembly_A_RES_79_239-EN.pdf
- United Nations Office for the Coordination of Humanitarian Affairs (OCHA) – occupied Palestinian territory, *The Humanitarian Monitor: OPT (October-November 2012) – OCHA report*, 2012, accessible at: https://www.un.org/unispal/document/auto-insert-201184/.
- United Nations Office for the Coordination of Humanitarian Affairs (OCHA), *Escalation in the West Bank of the Gaza Strip and Israel Flash Update #1 as of 17,00, 11 May 2021*, accessible at: https://www.ochaopt.org/content/escalation-west-bank-gaza-strip-and-israel-flash-update-1-1700-11-may-2021.
- United Nations Office for the Coordination of Humanitarian Affairs (OCHA), *West Bank: Escalation of Violence 13 April – 21 May 2021*, accessible at: https://www.ochaopt.org/content/west-bank-escalation-violence-13-april-21-may-2021.
- United Nations Office for the Coordination of Humanitarian Affairs (OCHA), *Protection of Civilians Report* | 24-31 May

2021, accessible at: https://www.ochaopt.org/poc/24-31-may-2021.

- United Nations Office for the Coordination of Humanitarian Affairs (OCHA), *Humanitarian Situation Update #275 | Gaza Strip, 27 Mar 2025*, accessible at: https://www.un.org/unispal/document/ocha-humanitarian-situation-update-275-gaza-strip/.
- United Nations Office of the High Commissioner for Human Rights (OHCHR), Pattern of Israeli attacks on Gaza hospitals raises grave converns – report, Dec. 31 2024, accessible at: https://www.ohchr.org/en/press-releases/2024/12/pattern-israeli-attacks-gaza-hospitals-raises-grave-concerns-report.
- United Nations Office of the High Commissioner for Human Rights (OHCHR), *Thematic Report: Attacks on hospitals during the escalation of hostilities in Gaza (7 October 2023-30 June 2024)*, Dec 31 2024, accessible at: https://www.ohchr.org/sites/default/files/documents/countries/opt/20241231-attacks-hospitals-gaza-en.pdf.
- United Nations Office of the High Commissioner for Human Rights (OHCHR), *Thematic Report: Indiscriminate and disproportionate attacks during the conflict in Gaza (October – December 2023)*, Jun 19 2024, accessible at: https://www.ohchr.org/sites/default/files/documents/countries/opt/20240619-ohchr-thematic-report-indiscrim-disprop-attacks-gaza-oct-dec2023.pdf.
- United Nations Support Mission in Libya (UNSMIL), *The Libyan Political Agreement*, signed in Skhirat, Morocco on 17 December 2015, accessible at: https://unsmil.unmissions.org/sites/default/files/Libyan%20Political%20Agreement%20-%20ENG%20.pdf.
- United Nations, Final Document of the Fifth Review Conference of the High Contracting Parties to the Convention on Certain Conventional Weapons, CCW/CONF.V/10, Geneva, 12-16 December 2016.
- United Nations, Meeting of the High Contracting Parties to the Convention on Certain Conventional Weapons: Final Report, CCW/MSP/2019/9, Geneva, 13-15 November 2019.

➢ DECISIONS AND OPINIONS OF THE INTERNATIONAL COURT OF JUSTICE

- International Court of Justice (ICJ), *Application of the Convention on the Prevention and Punishment of the Crime of Genocide in the Gaza Strip (South Africa v. Israel),* Order on the Request for the Indication of Provisional Measures, Jan 26 2024.
- International Court of Justice (ICJ), *Legal Consequences of Israel's Policies and Practices in the Occupied Palestinian Territory, including East Jerusalem*, Advisory Opinion, 19 Jul 2024.
- International Court of Justice (ICJ), *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 9 Jul 2004.
- International Court of Justice (ICJ), Legality of the Threat or Use of Nuclear Weapons, 1996, ICJ Rep 226.

➢ REPORTS, WORKING PAPERS, AND SUBMISSIONS TO THE GGE/CCW

- Belgium, *Intervention de la Belgique*, GGE, CCW, 2018, accessible at : https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2018/gge/statements/9April_Belgium.pdf.
- Group of Governmental Experts on Emerging Technologies in the Area of Autonomous Weapons Systems, *Position Paper Submitted by China*, CCW/GGE.1/2018/WP.7, 2018.
- Group of Governmental Experts on Emerging Technologies in the Area of Autonomous Weapons Systems, Switzerland, *A "Compliance-Based" Approach to Autonomous Weapon Systems*, Working Paper submitted to the GGE, CCW/GGE.1/2017/WP.9, 2017.
- Group of Governmental Experts on Emerging Technologies in the Area of Autonomous Weapons Systems, *Pakistan, Elements of an International Legal Instrument on Lethal*

Autonomous Weapons Systems (LAWS), Working Paper submitted to the GGE, CCW/GGE.1/2024/WP 7, 2024.

- ICRC, *Statement to the Convention on Certain Conventional Weapons (CCW) Meeting of Experts on Lethal Autonomous Weapons Systems,* 13-17 April 2015, Geneva, accessible at: https://www.icrc.org/en/document/lethal-autonomous-weapons-systems-LAWS.
- ICRC, *Views of the ICRC on autonomous weapon systems*, paper submitted to the Convention on Certain Conventional Weapons Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), Geneva 2016.
- Norway, *General Statement by Norway at the CCW*, Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), 13-17 November 2017.
- République Française, *Non Paper Characterization of a LAWS*, Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), Convention on Certain Conventional Weapons (CCW), 11–15 April 2016.
- State of Palestine, Submission on Autonomous Weapon Systems to the United Nations Secretary-General, 2024, accessible on: https://docs-library.unoda.org/General_Assembly_First_Committee_-Seventy-Ninth_session_%282024%29/78-241-State_of_Palestine-EN.pdf.
- The Netherlands, *Examination of Various Dimensions of Emerging Technologies in the Area of the Lethal Autonomous Weapons Systems*, Working Paper submitted to the GGE, CCW/GGE.1/2017/WP.2, 2017, accessible at: https://www.reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2017/gge/documents/WP2.pdf.

➢ **NATIONAL DOCUMENTS**

- Ministère des Armées (France), *Opinion on the Integration of Autonomy into Lethal Weapon Systems*, Defense Ethics Committee, 2021, accessible at: https://cd-geneve.delegfrance.org/IMG/pdf/defence_ethics_committee_-

_opinion_on_the_integration_of_autonomy_into_lethal_weapon_systems.pdf.

- Ministry of Defence (United Kingdom), *The Government Response to the Report by the House of Lords AI in Weapon Systems Committee: 'Proceed with Caution: Artificial Intelligence in Weapon Systems'*, Session 2023-24 HL paper 16, 2024, accessible at: https://assets.publishing.service.gov.uk/media/65cb77caa7ded0000c79e526/Government_response_to_the_House_of_Lords_AI_in_Weapon_Systems_Committee_Report.pdf.
- Ministry of Defence, *Joint Concept Note 1/18 : Human-Machine Teaming, Development, Concepts and Doctrine Centre*, United Kingdom, 2018.
- U.S. Department of Defense, *DoD Directive 3000.09: Autonomy in Weapon Sytems*, 2023.

➢ OTHERS

- Heyns, C., *Autonomous Weapons Systems and Human Rights Law*, Presentation made at the informal expert meeting organized by the state parties to the Convention on Certain Conventional Weapons, Geneva, 13-16 May 2014, accessible at: https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-_Informal_Meeting_of_Experts_(2014)/Heyns_LAWS_otherlegal_2014.pdf.
- ICRC, Customary IHL Database, accessible at: https://ihl-databases.icrc.org/en/customary-ihl.
- ICRC, *Practice relating to Rule 14. Proportionality in Attack*, accessible at: https://ihl-databases.icrc.org/en/customary-ihl/v2/rule14.
- International Criminal Court (ICC), *Statement of ICC Prosecutor Karim A.A. Khan KC: Applications for arrest warrants in the situation of the State of Palestine*, Office of the Prosecutor, 20 May 2024, accessible at: https://www.icc-

cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-applications-arrest-warrants-situation-state.

B. INSTITUTIONAL PUBLICATIONS

- Atlam, C., and Mekki, O., *Guide for Judges on International Humanitarian Law: Volume II*, ICRC, Geneva, 2015 (in Arabic).
- Atlam, H., *Lectures in International Humanitarian law*, ICRC, Cairo, 2010 (in Arabic).
- Bondar, K., *Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare*, Report, Center for Strategic & International Studies, 2025, accessible at: https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare#h2-introduction.
- Boulanin, V. and Verbruggen, M., *Mapping the Development of Autonomy in Weapon Systems,* Stockholm International Peace Research Institute (SIPRI), Sweden, 2017.
- Boulanin, V., Davison, N., Verbruggen, M., and Goussac, N., *Limits on Autonomy in Weapon Systems: Identifying Practical Elements of Human Control*, SIPRI and ICRC, 2020.
- Davison, N., *A legal perspective: Autonomous weapon systems under international humanitarian law*, UNODA Occasional Papers, No. 30, United Nations Office for Disarmament Affairs, 2018.
- Docherty B., *Shaking the Foundations The Human Rights Implications of Killer Robots*, Human Rights Watch and Harvard Law School International Human Rights Clinic, 2014, accessible at: https://www.hrw.org/report/2014/05/12/shaking-foundations/human-rights-implications-killer-robots.
- Gillis, M., *Disarmament A Basic Guide*, 4th ed., United Nations Office of Disarmament Affairs, New York, 2017.
- ICRC, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measure to Implement Article 36 of*

Additional Protocol I of 1977, Geneva, 2006, accessible at: https://www.icrc.org/en/publication/0902-guide-legal-review-new-weapons-means-and-methods-warfare-measures-implement-article.

- ICRC, *Artificial intelligence and machine learning in armed conflict: A human-centered approach*, International Review of the Red Cross, Digital technologies and war, vol 102, nº. 913, 2020.
- ICRC, *Autonomous weapon systems: Technical, military, legal and humanitarian aspects*, Expert meeting, Geneva, 26-28 March 2014.
- ICRC, *Autonomy, artificial intelligence and robotics : Technical aspects of human control*, 2019.
- ICRC, *ICRC Position on Autonomous Weapon Systems, Background Paper*, Geneva, 2021
- ICRC, *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*, Geneva, 2009, accessible at: https://www.icrc.org/en/publication/0990-interpretive-guidance-notion-direct-participation-hostilities-under-international.
- ICRC, *Libya: Use of Lethal Autonomous Weapon Systems*, ICRC Casebook, 2021, accessible at: https://casebook.icrc.org/case-study/libya-use-lethal-autonomous-weapon-systems.
- Puscas, I., *Human-Machine Interfaces in Autonomous Weapon Systems considerations for Human Control*, UNIDIR, 2022, accessible at: https://unidir.org/files/2022-07/UNIDIR_Human-Machine%20Interfaces.pdf.
- Rule, J. N., *A Symbiotic Relationship: The OODA Loop, Intuition, and Strategic Thought*, Strategy Research Project, United States Army War College, 2013, accessible at: https://apps.dtic.mil/sti/pdfs/ADA590672.pdf.
- Shaikh, S., and Rumbaugh, W., *The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense*, Center for Strategic & International Studies, 2020,

accessible at: https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense.

- Sokolski, H. D. (ed.), *Getting MAD: Nuclear Mutual Assured Destruction, Its Origins and Practice*, Strategic Studies Institute, 2004, accessible at: https://apps.dtic.mil/sti/tr/pdf/ADA428336.pdf.
- Surber, R., *Artificial Intelligence: Autonomous Technology (AT), Lethal Autonomous Weapons Systems (LAWS) and Peace Time Threats*, ICT for Peace Foundation and the Zurich Hub for Ethics and Technology (ZHET), 2018, accessible at: https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2018-AI-AT-LAWS-Peace-Time-Threats.pdf
- Thomas, A., *The Turkey-UAE race to the bottom in Libya: a prelude to escalation,* Fondation pour la Recherche Stratégique, Recherches & Documents, nº 8/2020.
- UNIDIR, *Algorithmic Bias and the Weaponization of Increasingly Autonomous Technologies: A primer*, UNIDIR Resources, nº. 9, 2018, accessible at: https://unidir.org/wp-content/uploads/2023/05/algorithmic-bias-and-the-weaponization-of-increasingly-autonomous-technologies-en-720.pdf.
- UNIDIR, *The Interpretation and Application of International Humanitarian Law to Lethal Autonomous Weapon Systems Background paper on the views of States, scholars and other experts*, 2025, accessible at: https://unidir.org/wp-content/uploads/2025/03/UNIDIR_The_Interpretation_and_Application_of_International_Humanitarian_Law_Lethal_Autonomous_Weapon_Systems.pdf.
- UNIDIR, *The Weaponization of Increasingly Autonomous Technologies: Concerns, Characteristics and Definitional Approches*, UNIDIR Resources No. 6, 2017.
- Williams, A. P., '*Defining Autonomy in Systems : Challenges and Solutions'*, in Andrew P. Williams and Paul D. Scharre (eds), *Autonomous Systems Issues for Defence Policymakers*, NATO Communications and Information Agency, The Netherlands, 2015.

C. ACADEMIC DOCTRINE

➢ BOOKS AND BOOK CHAPTERS

- Amer, S., *Introduction to the Study of the Law of Armed Conflicts*, Dar Al-Fekr Al-Arabi, Cairo, 1977 (in Arabic).
- Atlam, H., *Law of International Armed Conflicts*, Dar Al-Nahda Al-Arabia, 2003 (in Arabic).
- Bélanger, M., *Droit international humanitaire général*, Paris, Gualino, 2007 (in French).
- Cummings, M. L., *Automation Bias in Intelligent Time Critical Decision Support Systems*, in AIAA 1st Intelligent Systems Technical Conference, 20-22 Sep 2004, AIAA 2004-6313, accessible at: https://arc.aiaa.org/doi/10.2514/6.2004-6313.
- Fraden, J., *Handbook of Modern Sensors: Physics, Designs, and Applications*, 3rd ed., Springer, United States, 2004.
- Manovich, L., *Software Takes Command, International Texts in Critical Media Aesthetics*, Vol. 5, Bloomsbury Academic, 2013, Accessible at: https://library.oapen.org/bitstream/handle/20.500.12657/58738/9781623566722.pdf?sequence=1&isAllowed=y.
- McFarland, T., *Autonomous Weapon Systems and The Law of Armed Conflict: Compatibility with International Humanitarian Law,* Cambridge University Press, 2020.
- Pictet, J., *Développement et principes du droit international humanitaire*, Pedone, Paris, Institut Henry Dunant, Geneva, 1983 (in French).
- Roff, H., *Killing in war: Responsibility, liability, and lethal autonomous robots*, in F. Allhoff, N. Evans, and A. Henschke (eds.), *Routledge Handbook of Ethics and War: Just war theory in the 21st century*, Routledge, 2013.
- Safi Youssef, M., *The Mediator in International Humanitarian Law*, Dar Al-Nahda Al-Arabia, 2024 (in Arabic).

- Scharre, P., *Army of None : Autonomous Weapons and The Future of War*, W.W. Norton & Company, New York | London, 2018.
- Seixas-Nunes, A., *The Legality and Accountability of Autonomous Weapon Systems: A Humanitarian Law Perspective*, Cambridge University Press, 2022.
- Weller, M., *Introduction: International Law and the Problem of War*, in M. Weller (ed.), The Oxford Handbook of the Use of Force in International Law, Oxford University Press, 2015.

➢ JOURNAL ARTICLES

- Alwardt, C., and Krüger, M., *Autonomy of Weapon Systems*, Institute for Peace Research and Security Policy at the University of Hamburg (IFSH), 2016, accessible at: https://ifsh.de/file-IFAR/pdf_english/IFAR_FFT_1_final.pdf.
- Anderson, S. L., *Asimov's "Three Laws of Robotics" and Machine Metaethics, AI & Soc*, Springer Nature Link, Vol. 22, 2008, accessible at: https://link.springer.com/article/10.1007/s00146-007-0094-5
- Angelov, G., *Military Implications of the Nagorno-Karabkh Conflict: Tactics and Technologies*, Information & Security Journal, vol. 51, 2022, accessible at: https://isij.eu/system/files/download-count/2023-01/5104_nagorno-karabakh.pdf.
- Arkin, R., Governing *Lethal Behavior in Autonomous Robots*, Chapman and Hall/CRC press, New York, 2009.
- Arkin, R., *Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/Reactive Robot Architecture*, Technical Report GIT-GVU-07-11, Mobile Robot Laboratory, College of Computing, Georigia Institute of Technology, accessible at : https://sites.cc.gatech.edu/ai/robot-lab/online-publications/formalizationv35.pdf.
- Bächle, T. C., and Bareis, J., *"Autonomous weapons" as a geopolitical signifier in national power play: analysing AI imaginaries in Chinese and US military policies*, European Journal of Futures Research, SpringerOpen, 2022.

- Benson, S., *Prosecuting Asimov's Nightmare: Killer Robots and the Law of War*, Georgetown Security Studies Review, 2024, accessible at: https://georgetownsecuritystudiesreview.org/2024/03/04/prosecuting-asimovs-nightmare-killer-robots-and-the-law-of-war/.
- Christensen, E., *The Dilemma of Direct Participation in Hostilities*, Florida State University Journal of Transnational Law & Policy, Vol. 19, Issue 2, Article 2, 2010, accessible at: https://ir.law.fsu.edu/jtlp/vol19/iss2/2/.
- Crootof, R., *Autonomous Weapon Systems and the Limits of Analogy*, Harvard National Security Journal, Vol. 9, 2018, accessible at: https://harvardnsj.org/wp-content/uploads/2018/06/2_Crootof_LimitsOfAnalogy_06.08.18.pdf.
- Crootof, R., *The Killer Robots Are Here: Legal and Policy Implications,* Cardozo Law Review, Vol. 36 (1837), 2015.
- Crootof, R., *War Torts: Accountability for Autonomous Weapons*, University of Pennsylvania Law Review, Vol. 164, No. 6, 2016.
- Damar, M., Özen, A., Çakmak, U. E., Özoğuz, E., Erenay, F. S., *Super AI, Generative ai, Narrow AI and Chatbots: An Assessment of Artificial Intelligence Technologies for the Public Sector and Public Administration*, Journal of AI. Vol. 8(1), 2024.
- Demedziuk, S., *The New Dimension of War – The Ukraine Conflict*, Security and Defence Quarterly, 14(1), n.d., accessible at: https://securityanddefence.pl/pdf-105406-36134?filename=36134.pdf.
- Dhakal, A., and Borbin, B. D., *Cognitive Deficits*, StatPerls Publishing, PMID: 32644478, Excerpt, 2025 accessible at : https://pubmed.ncbi.nlm.nih.gov/32644478/.
- Dogra, A. K., Sharma, V., and Sohal, H., *A survey of deep learning techniques for detecting and recognizing objects in complex environments*, Computer Science Review, vol 54, 2024, accessible at:

https://www.sciencedirect.com/science/article/abs/pii/S1574013724000704.

- Etzioni, A., and Etzioni, O., *Pros and Cons of Autonomous Weapons Systems*, Military Review, 2017.
- Guanwan, Y., Aulawi, M. H., Anggriawan, R., and Putro, T. A., *Command responsibility of autonomous weapons under international humanitarian law*, Cogent Social Sciences, vol. 8(1), 2022, accessible at: https://repositori-api.upf.edu/api/core/bitstreams/8460a9ae-6c3a-4db2-91af-5c66f5be3613/content.
- Hayir, N., *Defining Weapon Systems with Autonomy: The Critical Functions in Theory and Practice*, Groningen Journal of International Law, vol. 9 (2): Open Issue, 2022.
- Hua, S., *Machine Learning Weapons and International Humanitarian Law: Rethinking Meaningful Human Control*, Georgetown Journal of International Law, [vol. 51], 2019.
- Jenks, C., *False Rubicons, Moral Panic, & Conceptual Cul-De-Sacs: Critiquing & Reframing the Call to Ban Lethal Autonomous Weapons*, Pepperdine Law Review, Vol. XLIV: 1, 2016.
- Jensen, E. T., *Autonomy and Precautions in the Law of Armed Conflict*, International Law Studies, vol. 96, 2020, accessible at: https://digital-commons.usnwc.edu/ils/vol96/iss1/19/.
- Li, S., He, X., Xu, X., Zhao, T., Song, C., and Li, J., *Weapon-target assignment strategy in joint combat decision-making based on multi-head deep reinforcement learning*, IEEE Access, 2023, accessible at: https://www.researchgate.net/publication/374693028_Weapon-Target_Assignment_Strategy_in_Joint_Combat_Decision-Making_based_on_Multi-head_Deep_Reinforcement_Learning.
- Liivoja, R., *Technological change and the evolution of the law of war*, International Review of the Red Cross, vol. 97, nº. 900, 2015.
- Liu, H.-Y., *Categorization and Legality of Autonomous and Remote Weapon Systems*, International Review of the Red Cross, Vol. 94, N. 886, 2012, accessible at :

https://international-review.icrc.org/sites/default/files/irrc-886-liu.pdf.

- Oimann, A.-K., *The Responsibility Gap and LAWS: a Critical Mapping of the Debate,* Philosophy & Technology, vol 36(1), article 3, 2023.
- Possati, L. M., *Towards a hermeneutic definition of software*, Humanities & Social Sciences Communications 7, 71, 2020, accessible at: https://www.nature.com/articles/s41599-020-00565-0#citeas.
- Postma, J., *Drones over Nagorno-Karabakh: A glimpse at the future of war?* JSTOR, 2021, accessible at: https://www.jstor.org/stable/pdf/48638213.pdf?refreqid=fastly-default%3A9dd091f496d7581327df34bc1a29bc26&ab_segments=&initiator=&acceptTC=1.
- Sassóli, M., *Autonomous Weapons and International Humanitarian Law: Advantages*, *Open Technical Questions and Legal Issues to be Clarified*, International Law Studies, U.S. Naval War College, Vol. 90, 2014, accessible at: https://digital-commons.usnwc.edu/ils/vol90/iss1/1/.
- Schmitt, M., *Autonomous Weapon Systems and International Humanitarian Law: A Reply to Critics*, Harvard National Security Journal, Vol. 4, 2013.
- Schmitt, M., *Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance*, Virginia Journal of International Law, vol. 50, no. 4, 2010.
- Schuller, A. L., *At the Crossroads of Control: The Intersection of Artificial Intelligence in Autonomous Weapon Systems with International Humanitarian Law*, Harvard National Security Journal, Vol. 8, 2017.
- Sharkey, N., *The human control of weapons: a humanitarian perspective*, in N. Bhuta, S. Beck, R. Geiss, C. Kress, H. Y. Liu (eds.), *Autonomous Weapons Systems: Law, Ethics, Policy*, Cambridge University Press, Draft version, accessible at: https://archive.law.upenn.edu/live/files/3948-sharkey---human-control-of-weapons-pf-draftpdf.

- Sotoudehfar, S., *Drone on the frontline: Charting the use of drones in the Russo-Ukrainian Conflict and how their use may be violating international humanitarian law*, International and Comparative Law Review, vol. 23, no. 2, 2023, accessible at: https://sciendo.com/article/10.2478/iclr-2023-0018.
- Sparrow, R., *"Killer Robots"*, Journal of Applied Philosophy, vol. 24, no. 1, 2007, accessible at: : http://www.jstor.org/stable/24355087.
- Sun, H., *Image Target Detection and Recognition Method Using Deep Learning, Advances in Multimedia*, vol. 2022, Issue 1, 2002, accessible at: https://onlinelibrary.wiley.com/doi/10.1155/2022/4751196.
- Thompson, M., *Beyond The Battlefield: Navigating The Future of AI and Autonomous Systems in Electronic Warfare*, The Journal of Electromagnetic Dominance, 2024, accessible at: https://www.jedonline.com/2024/05/06/beyond-the-battlefield-navigating-the-future-of-ai-and-autonomous-systems-in-electronic-warfare/.
- Whelan, C., *The 2020 Nagorno Karabakh War: Unmanned Combat Aerial Vehicles in Modern Warfare*, Air and Space Power Review, vol. 24 no. 2, 2023, accessible at: https://www.raf.mod.uk/what-we-do/centre-for-air-and-space-power-studies/aspr/aspr-vol25-iss2-3-pdf/.
- Wilmes, L., and Waas, R. V., *Understanding Arms Races for Autonomous Military Capabilities Using a System Dynamics Simulation Model*, Nato STO Review Spring 2024, accessible at: https://review.sto.nato.int/images/Papers/Peer_Review_Journal_4_Spring_2024_21-Wilmes.pdf.
- Winter, E., *The Compatibility of Autonomous Weapons with the Principles of International Humanitarian Law*, Journal of Conflict & Security Law, Oxford University Press, 2022.
- Zając, M., *AWS compliance with the ethical principle of proportionality: Three possible solutions*, Ethics and Information Technology, Vol. 25, article 13, 2023, accessible at: https://link.springer.com/article/10.1007/s10676-023-09689-8.

➢ MASTER'S AND PHD THESES

- Ekelhof, M., *The Distributed Conduct of War: Reframing Debates on Autonomous Weapons, Human Control and Legal Compliance in Targetin*g, PhD-Thesis, Vrije Universiteit Amsterdam, 2019, accessible at: https://research.vu.nl/ws/portalfiles/portal/90547665/complete%20dissertation.pdf.
- Fisher, A. B., *How international humanitarian law will constrain the use of autonomous weapon systems in the conduct of hostilities*, Masters Thesis, Murdoch University, 2022, accessible at: https://researchportal.murdoch.edu.au/esploro/outputs/graduate/How-international-humanitarian-law-will-constrain/991005542029107891/filesAndLinks?index=0
- Homayounnejad, M., *Lethal Autonomous Weapon Systems Under the Law of Armed Conflict*, PhD Thesis, King's College London, 2018, accessible at: https://kclpure.kcl.ac.uk/ws/portalfiles/portal/110384075/2019_Homayounnejad_Maziar_0222601_ethesis.pdf.
- Posthuma, D.-J., *Autonomous Weapons Systems and Command Responsibility: Addressing the Specter of Impunity*, Master Thesis, Tilburg University, 2019, accessible at: https://arno.uvt.nl/show.cgi?fid=149083.

➢ ACADEMIC BLOGS AND OTHER SOURCES

- Amnesty International, *Israel's Occupation: 50 Years of Dispossession*, 2017, accessible at: https://www.amnesty.org/en/latest/campaigns/2017/06/israel-occupation-50-years-of-dispossession/.
- Anjum, H., *Second Libyan Civil War (2014-2020): Causes and Impacts*, n.p., 2022, accessible at: https://www.researchgate.net/publication/366445100_SECOND_LIBYAN_CIVIL_WAR_2014-2020_CAUSES_AND_IMPACTS.

- Bendett, S., and Kirichenko, D., *Ukraine Symposium – The Continuing Autonomous Arms Race*, Lieber Institute West Point, 2025, accessible at: https://lieber.westpoint.edu/continuing-autonomous-arms-race/.
- Chávez, K., and Swed, O., *How Hamas innovated with drones to operate like an army*, Bulletin of the Atomic Scientists, 2023, accessible at: https://thebulletin.org/2023/11/how-hamas-innovated-with-drones-to-operate-like-an-army/.
- Davison, N., *Autonomous weapon systems: An ethical basis for human control*, ICRC Humanitarian Law & Policy Blog, 2018, accessible at: https://blogs.icrc.org/law-and-policy/2018/04/03/autonomous-weapon-systems-ethical-basis-human-control/.
- Ekelhof, M., *Autonomous Weapons: Operationalizing Meaningful Human Control*, ICRC Humanitarian Law & Policy Blog, 2018, accessible at: https://blogs.icrc.org/law-and-policy/2018/08/15/autonomous-weapons-operationalizing-meaningful-human-control/.
- Hong-Peng, Z., *Maneuver Decision-Making Through Automatic Curriculum Reinforcement Learning Without Handcrafted Reward functions*, arXiv, 2023, accessible at: https://arxiv.org/pdf/2307.06152.
- Kashif, M., Arslan, M., Chakma, R., Banoori, F., Al Mamun, A., Chakma, G. L., *Design and Implementation of Image Capture Sentry Gun Robot*, MATEC Web of Conferences, 160, 06007, 2018, accessible at: https://www.matec-conferences.org/articles/matecconf/pdf/2018/19/matecconf_eecr2018_06007.pdf.
- Khachatryan, D., *Complete Defeat and the End of the Non-Recognized State of Nagorno-Karabak*, Lieber Institute West Point, Articles of War, 2024, accessible at: https://lieber.westpoint.edu/complete-defeat-end-non-recognized-state-nagorno-karabakh/.
- Kirichenko, D., *Drone superpower: Ukrainian innovation offers lessons for NATO*, Atlantic Council Blog, 2025, accessible at:

https://www.atlanticcouncil.org/blogs/ukrainealert/drone-superpower-ukrainian-wartime-innovation-offers-lessons-for-nato/.

- Lee, H., Park, S., Yun, W. J., Jung, S., and Kim, J., *Situation-aware deep reinforcement learning for autonomous nonlinear mobility control in cyber-physical loitering munition systems*, arXiv, 2022, accessible at: https://arxiv.org/pdf/2301.00124.
- Nasu, H., *The Kargu-2 Autonomous Attack Drone: Legal & Ethical Dimensions*, Lieber Institute West Point, 2021, accessible at: https://lieber.westpoint.edu/kargu-2-autonomous-attack-drone-legal-ethical/.
- Nilson, N. J., *Introduction to Machine Learning: An Early Draft of a Proposed Textbook*, Robotics Laboratory, Department of Computer Science, Standford University, 1998, accessible at: https://ai.stanford.edu/~nilsson/MLBOOK.pdf.
- Roff, H., *Distinguishing autonomous from automatic weapons*, Bulletin of the Atomic Scientists, 2016, accessible at: https://thebulletin.org/roundtable_entry/distinguishing-autonomous-from-automatic-weapons/.
- Sparrow, R., *Ethics as a source of law: The Martens clause and autonomous weapons*, ICRC Humanitarian Law & Policy Blog, 2017, accessible at: https://blogs.icrc.org/law-and-policy/2017/11/14/ethics-source-law-martens-clause-autonomous-weapons/.
- Trabucco, L., *What is Meaningful Human Control, Anyway? Cracking the Code on Autonomous Weapons and Human Judgment*, Modern War Institute at West point, 2023, accessible at: https://mwi.westpoint.edu/what-is-meaningful-human-control-anyway-cracking-the-code-on-autonomous-weapons-and-human-judgment/.

D. OTHER SOURCES

➢ DICTIONARIES AND ENCYCLOPEDIAS

- Cambridge Dictionary, Cambridge University Press, accessible at: https://dictionary.cambridge.org.
- Haskar, V., Moral Agents, in *The Routledge Encyclopedia of Philosophy,* Taylor and Francis, 1998, accessible at: https://www.rep.routledge.com/articles/thematic/moral-agents/v-1.
- ICRC, Glossary, ICRC Casebook: https://casebook.icrc.org/a_to_z.
- Médecins Sans Frontières, *The Practical Guide to Humanitarian Law*, "Weapons, Categories of Weapons", accessible at : https://guide-humanitarian-law.org/content/article/3/weapons/.
- Merriam-Webster Dictionary, accessible at: https://www.merriam-webster.com.
- The Editors of Encyclopaedia Britannica, "Three laws of robotics", Encyclopedia Britannica, 2025, accessible at : https://www.britannica.com/topic/Three-Laws-of-Robotics.

➢ NEWS AND INVESTIGATIVE REPORTS

- Abraham, Y., *'A mass assassination factory': Inside Israel's calculated bombing of Gaza*, Investigative Report, 30 Nov 2023, accessible at: https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/.
- Abraham, Y., '*Lavender': The AI machine directing Israel's bombing spree in Gaza*, +972 Magazine, Investigative Report, 3 Apr 2024, accessible at: https://www.972mag.com/lavender-ai-israeli-army-gaza/.
- Ackerman, S., *Israel's Armed Quadcopters in Gaza Mark a Dangerous New Era in Drone Warfare*, Zeteo, 29 Apr 2024, accessible at: https://zeteo.com/p/israel-gaza-quadcopter-drone-warfare.
- AlJazeera, *'Brief skirmish' near Libya's Tripoli as Haftar's LNA heads west*, 4 Apr 2019, accessible at:

https://www.aljazeera.com/news/2019/4/4/brief-skirmish-near-libyas-tripoli-as-haftars-lna-heads-west.

- AlJazeera, *Israel retrofitting DJI commercial drones to bomb and surveil Gaza*, 8 May 2025, accessible at: https://www.aljazeera.com/news/2025/5/8/israel-retrofitting-dji-commercial-drones-to-bomb-and-surveil-gaza.
- AlJazeera, *Timeline: Haftar's months-long offensive to seize Tripoli*, 19 Feb 2020, accessible at: https://www.aljazeera.com/news/2020/2/19/timeline-haftars-months-long-offensive-to-seize-tripoli.
- Army Recognition, *Ukrainian Drones Destroyed 88 Russian Tanks This Month in Two-Week Technological Blitz*, 2024, accessible at: https://armyrecognition.com/focus-analysis-conflicts/army/conflicts-in-the-world/russia-ukraine-war-2022/ukrainian-drones-destroyed-88-russian-tanks-this-month-in-two-week-technological-blitz?highlight=WyJydXNzaWEiXQ%3D%3D.
- Associated Press News (AP News), *Drone advances in Ukraine could bring dawn of killer robots*, 9 May 2023, accessible at: https://apnews.com/article/russia-ukraine-war-drone-advances-6591dc69a4bf2081dcdd265e1c986203.
- BBC, "Stanislav Petrov : The man who may have saved the world", BBC News, 26 Sep 2013, accessible at : https://www.bbc.com/news/world-europe-24280831.
- BBC, *Israel and the Palestinians: History of the conflict explained*, 2025, accessible at: https://www.bbc.com/news/newsbeat-44124396.
- BBC, *Nagorno-Karabakh: President Ilham Aliyev speaks to the BBC*, Televised Interview, 9 Nov. 2020, accessible at: https://www.bbc.com/news/av/world-europe-54865589.
- Chen, G., Opinion | *In AI race against US, China is racking up real-world wins*, 2025, accessible at: https://www.scmp.com/opinion/china-opinion/article/3307357/ai-race-against-us-china-racking-real-world-wins.
- CNN, *How Ukraine became a testbed for Western weapons and battlefield innovation*, 15 Jan 2023, accessible at:

https://edition.cnn.com/2023/01/15/politics/ukraine-russia-war-weapons-lab.

- Cohen, S., *Shark Tanks: With Gaza as Testing Ground, Israeli Defense Startups Flourish*, HAARETZ, 3 Jan 2024, accessible at: https://www.haaretz.com/israel-news/2024-01-03/ty-article-magazine/.premium/suicide-drones-and-ai-with-gaza-as-testing-ground-israeli-defense-startups-flourish/0000018c-cf39-ddba-abad-cfb9a3ee0000.
- Copp, T., *Kyiv Asked for a New Kamikaze Drone to Fight Russia. The Air Force Delivered Phoenix Ghost*, Science & Tech, Defense One, 2022, accessible at: https://www.defenseone.com/technology/2022/04/kyiv-asked-new-kamikaze-drone-fight-russia-air-force-delivered-phoenix-ghost/365945/.
- Dogson, L., *Hamas used drone bombs to launch its war on Israel from Gaza, and took out hi-tech observation towers, videos show*, Business Insider, 8 Oct 2023, accessible at: https://www.businessinsider.com/video-hamas-used-drone-bombs-to-launch-war-with-israel-2023-10?r=US&IR=T.
- Freedberg JR, S. J., *Trained on classified battlefield data, AI multiplies effectiveness of Ukraine's drones*: *Report*, 2025, accessible at: https://breakingdefense.com/2025/03/trained-on-classified-battlefield-data-ai-multiplies-effectiveness-of-ukraines-drones-report/.
- Gigova, R., "*Who Vladimir Putin thinks will rule the world*," CNN, 2017, accessible at: https://edition.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html.
- Human Rights Watch, *Azerbaijan: Unlawful Strikes in Nagorno-Karabakh Investigate Alleged Indiscriminate Attacks, Use of Explosive Weapons*, Report, 2020, accessible at: https://www.hrw.org/news/2020/12/11/azerbaijan-unlawful-strikes-nagorno-karabakh.
- Iddon, P., *Turkey and Israel Upgrade Azerbaijan's Russian Military Hardware*, Forbes, 2024, accessible at: https://www.forbes.com/sites/pauliddon/2024/10/09/turkey-and-israel-upgrade-azerbaijans-russian-military-hardware/.

- Israel Defense, *לראשונה נחשף: כך פועלת מערכת הבינה המלאכותית של צה"ל במבצעי סיכול ממוקד* [For the first revealed: How the IDF's artificial intelligence system operates in targeted operations], Nov 10 2022, available in Hebrew at: https://www.israeldefense.co.il/node/57256#google_vignette .
- Jankowicz, M., *How Hamas likely used rudimentary drones to 'blind and deafen' Israel's border and pave the way for its onslaught,* Business Insider, 10 Oct 2023, accessible at: https://www.businessinsider.com/hamas-drones-take-out-comms-towers-ambush-israel-2023-10.
- Kuzio, T., *Western Weapons Made the Difference in Ukraine and the Second Karabakh War*, Geopolitical Monitor, Opinion, 2024, accessible at: https://www.geopoliticalmonitor.com/western-weapons-made-the-difference-in-ukraine-and-the-second-karabakh-war/.
- Lonsdorf, K., *Eyewitnesses in Gaza say Israel is using spiner drones to shoot Palestinians*, NPR, 26 Nov 2024, accessible at: https://www.npr.org/2024/11/26/g-s1-35437/israel-sniper-drones-gaza-eyewitnesses.
- Ministry of Foreign Affairs (Israel), *Swrods of Iron: Hostages and Missing Persons Report,* 2023, updated 12 May 2025, accessible at: https://www.gov.il/en/pages/hostages-and-missing-persons-report
- Quds News Network (QNN) | Just International, *Israel Uses Suicide Drones Against Gatherings of Displaced Families*, 22 Apr 2025, accessible at: https://just-international.org/articles/israel-uses-suicide-drones-against-gatherings-of-displaced-families/.
- Reuters, *Israel revises Hamas attack death toll to 'around 1200'*, 10 Nov 2023, accessible at: https://www.reuters.com/world/middle-east/israel-revises-death-toll-oct-7-hamas-attack-around-1200-2023-11-10/.
- Reuters, *Ukraine ramps up arms production, can produce 4 million drones a year, Zelensky says*, 2 October 2024, accessible at: https://www.reuters.com/world/europe/ukraine-

ramps-up-arms-production-can-produce-4-million-drones-year-zelenskiy-2024-10-02/.

- Roblin, S., *What Open Source Evidence Tells Us About The Nagorno-Karabakh War*, Forbes, 2020, accessible at: https://www.forbes.com/sites/sebastienroblin/2020/10/23/what-open-source-evidence-tells-us-about-the-nagorno-karabakh-war/.
- Sapwood, O., *In the south of Ukraine, the Bayraktar TB2 drone neutralized the tanks of the Russian Federation*, MILITARNY, 2022, accessible at: https://militarnyi.com/en/news/in-the-south-of-ukraine-the-bayraktar-tb2-drone-neutralized-the-tanks-of-the-russian-federation/.
- Satam, P., *Hamas reveals "Zouari" kamikaze drone that can potentially rain hell on israel During Gaza Ops*, The EurAsian Times, 12 Oct 2023, accessible at: https://www.eurasiantimes.com/hamas-reveals-zouari-kamikaze-drone-that-can-potentially-rain/.
- The Guardian, *A visual guide to the destruction of Gaza*, 18 Jan 2025, accessible at: https://www.theguardian.com/world/2025/jan/18/a-visual-guide-to-the-destruction-of-gaza.
- The Guardian, *Israel Defence Forces' response to claims about the use of 'Lavender' AI database in Gaza*, Apr 3 2024, accessible at: https://www.theguardian.com/world/2024/apr/03/israel-defence-forces-response-to-claims-about-use-of-lavender-ai-database-in-gaza.
- The Libya Observer, *Libyan Army launches Operation Peace Storm against Haftar's attacks on civilians*, 25 March 2020, accessible at: https://libyaobserver.ly/news/libyan-army-launches-operation-peace-storm-against-haftars-attacks-civilians.
- The Washington Post, *Israel built an 'AI factory' for war. It unleashed it in Gaza*, 29 Dec 2024, accessible at: https://www.washingtonpost.com/technology/2024/12/29/ai-israel-war-gaza-idf/.

- Top War, *The losses of military equipment of the Armenian Armed Forces in Nagorno-Karabakh assessed in Baku*, Military Review News, 2 Dec. 2020, accessible at: https://en.topwar.ru/177706-v-baku-ocenili-poteri-voennoj-tehniki-vs-armenii-vo-vremja-vojny-v-nagornom-karabahe.html.
- WIRED, *Russia's Killer Drone in Ukraine Raises Fears About AI in Warfare*, 2022, accessible at: https://www.wired.com/story/ai-drones-russia-ukraine/.

➢ WEBSITES

- Army Guide, *Super aEgis II*, n.d., accessible at: https://www.army-guide.com/eng/product4914.html.
- Army Technology, *Zala KYB Strike Drone, Russia*, 2023, accessible at: https://www.army-technology.com/projects/zala-kyb-strike-drone-russia/.
- Automated Decision Research, *State positions on Autonomous Weapons*, n.d., accessible at : https://automatedresearch.org/state-positions/?_state_position_negotiation=yes.
- Automated Decision Research, *Weapons Systems with autonomous functions used in Ukraine*, n.d., accessible at: https://automatedresearch.org/news/weapons-systems-with-autonomous-functions-used-in-ukraine/.
- AVINC, *Switchblade 300 Block 20*, n.d. ,accessible at: https://www.avinc.com/lms/switchblade ,
- AVINC, *Switchblade 600*, n.d., accessible at: https://www.avinc.com/lms/switchblade-600.
- Brown, S., *Machine learning, explained*, MIT Management Sloan School of Management, 2021, accessible at: https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained.
- Carpenter, C., "*Robot Soldiers Would Never Rape": Un-packing the Myth of the Humanitarian War-Bot,* 2014, accessible at:

https://www.duckofminerva.com/2014/05/robot-soldiers-would-never-rape-un-packing-the-myth-of-the-humanitarian-war-bot.html.

- Center for Preventive Action, *Civil Conflict in Libya*, Global Conflict Tracker, 2024, accessible at: https://www.cfr.org/global-conflict-tracker/conflict/civil-war-libya.
- Coalition for Critical Technology, *Abolish the Tech-to-Prison Pipeline*, 23 Jun 2020, accessible at : https://medium.com/@CoalitionForCriticalTechnology/abolish-the-techtoprisonpipeline-9b5b14366b16.
- Council on Foreign Relations, *Israeli-Palestinian Conflict Timeline*, 2024, accessible at: https://education.cfr.org/learn/timeline/israeli-palestinian-conflict-timeline.
- Fatafta, M., and Leufer, D., *Artificial Genocidal Intelligence: how Israel is automating human rights abuses and war crimes*, Access Now, 9 May 2024, accessible at: https://www.accessnow.org/publication/artificial-genocidal-intelligence-israel-gaza/#:~:text=fully%20automated%20“killer%20robots”%20on,driven%20horrors.
- Geraghty, T., *John Boyd and The OODA Loop*, Psych Safety, 2024, accessible at: https://psychsafety.com/john-boyd-and-the-ooda-loop/.
- Holdsworth, J., *What is deep learning?* IBM, 2024, accessible at: https://www.ibm.com/think/topics/deep-learning.
- IBM, *Understanding the different types of artificial intelligence*, 2023, accessible at: https://www.ibm.com/think/topics/artificial-intelligence-types.
- LINAK, *What is an actuator?* 2024, accessible at : https://www.linak.com/products/linear-actuators/what-is-an-actuator/
- Pal, S., *Autonomous Combat Systems: Challenges and Opportunities in Land, Air, and Sea*, Medium, 2023, accessible at: https://medium.com/@siam_VIT-

B/autonomous-combat-systems-challenges-and-opportunities-in-land-air-and-sea-74d554a926a.

- Rao, R., *What are End Effectors? Types of End Effectors in Robotics and Applications*, Wevolver, 2024, accessible at: https://www.wevolver.com/article/end-effector.
- Stop Killer Robots, *Facts about Autonomous Weapons*, n.d., accessible at: https://www.stopkillerrobots.org/stop-killer-robots/facts-about-autonomous-weapons/.
- Stop Killer Robots, *Growing Consensus on Policy at UN Discussions on AWS but Skepticism Towards Non-Binding Principles & Practices*, 2022, accessible at: https://www.stopkillerrobots.org/news/growing-consensus-on-policy-at-un-discussions/.
- Syracuse University School of Information Studies, *Types of AI: Explore Key Categories and Uses*, 2025, accessible at: https://ischool.syracuse.edu/types-of-ai/.
- Taclia, *What is Software? Definition, types and examples of use*, 2025, accessible at: https://www.taclia.com/en-us/blog/what-is-software.
- TVD.IM, *IAI Rotem L*, n.d., accessible at: https://tvd.im/aviation/1089-iai-rotem-l.html.
- U.S. Navy, *MK15 Phalanx Close-In Weapon System (CIWS)*, Navy.mil, Fact Files, 2021, accessible at: https://www.navy.mil/resources/fact-files/display-factfiles/article/2167831/mk-15-phalanx-close-in-weapon-system-ciws/.
- United Nations | The Question of Palestine, *History of the question of Palestine*, n.d., accessible at: https://www.un.org/unispal/history/.