Brooklyn Journal of International Law

Volume 46 | Issue 2 Article 3

12-1-2021

Autonomous Weapons Systems and the Procedural Accountability Gap

Afonso Seixas-Nunes

AUTONOMOUS WEAPONS SYSTEMS AND THE PROCEDURAL ACCOUNTABILITY GAP

Afonso Seixas-Nunes, sj[*]

INTRODUCTION

Cicero, in *Pro Milone*, argued that *inter arma silent leges.*[1] The expression used by Cicero is traditionally translated

---

[*] Assistant Professor of Law at Saint Louis University School of Law (SLU). This article was written as a Postdoctoral Student at the Oxford Institute for Ethics, Law and Armed Conflict (ELAC). Junior Research fellow at Campion Hall (University of Oxford). The author would sincerely like to thank Antonio Coco; Professor Carlos Vasquez; Daragh Murray; Filipe Avides Moreira; Natalia Jevgleskaja; Nathan Derejko; Rain Liivoja and Russell Buchan, for helpful comments on previous drafts.

1. Marcus Tullius Cicero, Pro Milone 5 (1980).

as "in the times of war, laws fall silent", but a more literal translation of that expression reads as "for among arms, the laws fall mute."[2] This quotation is very much at the root of this study, as it seeks to explain how International Humanitarian Law (IHL) is not *silent* regarding the future deployment of Autonomous Weapon Systems (AWS). As certain is this may be, the reality is that States fail to comply with important obligations on matters of technology of warfare. This situation does not portend bright future if AWS are deployed in the battlefield for the reasons explored in this article.

IHL is a branch of International Law that must be distinguished from the law on the prohibition of use of force (*Jus ad Bellum*), which is regulated by the United Nations Charter (UNC).[3] IHL, also known as *Jus in Bello*, does not prohibit the use of armed force but seeks to limit the use of violence between the parties in an armed conflict.[4] Therefore, it intends to protect those who do not or no longer directly participate in hostilities, civilian objects, and limits the right of parties to the conflict to use armed force only to the extent necessary to achieve the aim of the conflict, which is to weaken the military potential of the enemy.[5] The development and well-established principles of IHL have been progressively establishing limits to the means and methods of warfare and dictating obligations to the parties in armed conflicts, frustrating Cicero's pessimism.[6]

---

2. Oxford Treasury of Sayings and Quotations, 484 (17) (Susan Ratcliffe ed., 4th ed. 2011).

3. Olivier Corten, The Law Against War: The Prohibition on the Use of Force in Contemporary International Law, 4 Fr. Stud. Int'l L. 50 (Cristopher Sutcliffe trans., 2012) (2008); Nils Melzer, International Humanitarian Law: A Comprehensive Introduction 27 (Etienne Kuster ed., 2019).; Christine Gray, International Law and the Use of Force 30 (4th ed. 2018).

4. Melzer, SUPRA note 3, at 17.

5. Jann K. Kleffner, SCOPE OF APPLICATION OF INTERNATIONAL HUMANITARIAN LAW, IN The Handbook of Int'l Humanitarian L. 43, 43 (Dieter Fleck ed., 3d ed. 2013); Marco Sassoli, International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare 1.01–1.05 (2019); Jean-Marie Henckaerts, HISTORY AND SOURCES, IN The Oxford Guide to International Humanitarian Law 1, 1–2 (Ben Saul & Dapo Akande eds., 2020).

6. Melzer, SUPRA note 3, at 17–20. SEE ALSO Michael N. Schmitt, INTERNATIONAL HUMANITARIAN LAW AND THE CONDUCT OF HOSTILITIES,

This article aims to expand the academic reflection upon AWS from a more pragmatic angle. Beyond the presently available solutions, this article aims to identify problems that, to the author's best knowledge, have not received the attention they deserve. On one hand, the technical side of AWS has been neglected by scholars, especially regarding how that dimension can affect State responsibility. On the other, little attention has been given to how States behave towards their international obligations as far as weapons are concerned. Thus, this article is divided in two different, but complementary, parts. Part I aims to look at the technical complexity of the algorithms embedded with AWS. Machine-Learning Algorithms (MLA), namely neural networks, are one of the most recent advances in the field of Artificial Intelligence (AI) and are known to be inherently unpredictable.[7] From this unpredictability, it follows that AWS can commit *errors* for which no one can be held accountable—except the deploying State. Weapons' malfunctions are not unknown on the battlefield but with the advent of AWS, MLA are now entrusted with the selection-making process of military targets without human intervention. If the AWS's software results in a targeting *error* that causes an unlawful, unpredictable outcome, vital to attribute responsibility to the deploying State.

Once the category of *error* is accepted and the responsibility of the deploying State is explained, Part II of this article will focus on the obligations of States with particular relevance for the future introduction of AWS on the battlefield. Thus, it focusses on procedural aspects of States' obligations regarding IHL, in general, and new weapons, in particular. In this context, Common Article 1 to the 1949 Geneva Conventions (Common Article 1)[8]—the obligation of States to "respect" and "ensure respect" for IHL

IN The Oxford Guide to International Humanitarian Law 147, 147–74 (Ben Saul & Dapo Akande eds., 2020).

7. SEE GENERALLY David Danks, LEARNING, IN The Cambridge Handbook of Artificial Intelligence 151, 151–67 (Keith Frankish & William M. Ramsey eds., 2014); Int'l Comm. of the Red Cross (ICRC), Autonomy, Artificial Intelligence and Robotics: Technical Aspects of Human Control ¶¶ 4, 7 (2019).

8. Int'l Comm. Red Cross (ICRC), Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, https://www.icrc.org/en/doc/assets/files/publications/icrc-002-0173.pdf.

in all circumstances—and Article 36 of the 1977 Additional Protocol I (API)[9]—States' obligation to proceed to legal reviews of AWS—require special attention. As the article unfolds, there will be the opportunity to demonstrate that States' commitment towards IHL falls short of what would be expected. Looking at the practice of States in matters of weaponry, it is possible to conclude that States *fall silent* with their obligations compromising the operationality of IHL. This reality allows this article to revisit the expression by Cicero by arguing that in times of arms, States fall silent.

I. INTRODUCING AWS AND THE CURRENT INTERNATIONAL DEBATE

The idea of autonomous systems, which depend exclusively on their embedded algorithms and do not require human intervention, has caught the imagination and excitement of many. State armed forces have been using weaponry with limited autonomy for some time now.[10] At present, however, such weapons are only

9. Int'l Comm. of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreaties1949.xsp.

10. SEE Ronald C. Arkin, Governing Lethal Behavior in Autonomous Robots, 7–26 (2009) (Several automatic and semi-autonomous systems are already operating and use by States such Samsung Sentris, Iron Dume, AEGIS and the Brimstone Missile, among others); SEE ALSO EU STATEMENT ON LETHAL AUTONOMOUS WEAPONS SYSTEMS (LAWS) Group of Governmental Experts, Convention on Certain Conventional Weapons, (Nov. 13–17, 2017) (As Governmental Experts from EU, the UK and the USA have reinforced in the discussions held in Geneva, such systems should not be confused with "lethal autonomous weapons"); STATEMENT FOR THE GENERAL EXCHANGE OF VIEWS AT THE MEETING OF THE GROUP OF GOVERNMENT EXPERTS ON LETHAL AUTONOMOUS WEAPONS SYSTEMS, U.K, and N. Ir. Commw. Off. (Apr. 9, 2018), https://www.unog.ch/80256EDD006B8954/(httpAssets)/271A66FCD9412E18C125827A003454CF/$file/2018_LAWSGeneralExchange_UK.pdf.; SEE ALSO Michael W. Meier, U.S. Opening Statement Delivered at the Convention on Certain Conventional Weapons (CCW) Informal Meeting of Experts on Lethal Autonomous Weapons Systems, Geneva (Apr. 13, 2015), https://geneva.usmission.gov/2015/04/15/u-s-opening-statement-at-the-ccw-informal-meeting-of-experts-on-lethal-autonomous-weapons-systems/.

capable of identifying pre-determined military targets.[11] Autonomous systems would represent, therefore, a total shift in the way war has been conducted. Human agents would become, at most, "supervisors" of how AWS perform on the battlefield.

Today's AI systems are based on machine learning and, when combined with recent advances in the manufacture of hardware, create the perfect technological environment for the development of AWS; but this will not come about without challenges and difficulties.[12] Since 2014 several meetings have been held at *The Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be Deemed to be Excessively Injurious or to Have Indiscriminate Effects* (CCW) to discuss the reality and future of AWS.[13] Little consensus, however, has been achieved among scholars, States' delegates, and governmental experts regarding apparently simple problems such as the *definition* of AWS.[14] To the present day, more than 25

---

11. SEE BRIMSTONE ADVANCE ANTI-ARMOUR MISSILE, Army Technology, https://www.army-technology.com/projects/brimstone/ (A perfect example is the Brimstone Missile which in indirect mode searches autonomously for armour vehicles).

12. Wojchiech Samek & Klaus-Robert Muller, TOWARDS EXPLAINABLE ARTIFICIAL INTELLIGENCE, IN Explainable AI: Interpreting, Explaining and Visualizing Deep Learning 5, 6 (Wojciech Samek et. al. eds., 2019); SEE ALSO Vincent Boulanin & Maaike Verbruggen, Mapping the Development of Autonomy in Weapon Systems 23 (2017), https://www.sipri.org/sites/default/files/2017-11/siprireport_mapping_the_development_of_autonomy_in_weapon_systems_1117_1.pdf; Danny Zhu & Manuela Veloso, VIRTUALLY ADAPTED REALITY AND ALGORITHM VISUALIZATION FOR AUTONOMOUS ROBOTS, 20th RoboCup Int'l Symp., Leipzig, Germany (2016), http://www.ais.uni-bonn.de/robocup.de/2016/papers/RoboCup_Symposium_2016_Zhu.pd.

13. The United Nations Office at Geneva, CCW - 2014 MEETINGS, https://www.unog.ch/80256EE600585943/(httpPages)/A038DEA1DA906F9DC1257DD90042E261?OpenDocument (2020).

14. SEE GENERALLY Second Review Conf. of the States Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, Geneva, U.N. Doc. A/CONF.95/CW/SR.13 (Oct. 7, 1980) (The CCW was adopted to restrict weapons "considered to cause unnecessary or unjustifiable suffering to combatants or to affect civilians indiscriminately." While the CCW's Protocols initially only applied to international armed conflicts, since the Second Review Conference in 2001, the CCW's scope

countries, including Algeria, Argentina, Austria, China,[15] Ecuador, the Holy See, Iraq, and others,[16] and 100 nongovernmental organizations, including Amnesty International, Human Rights Watch, and Pax International, among others, have called for a pre-emptive ban of AWS on account of pervasive questions regarding ethics and accountability, as well as the unlikelihood

---

of application has been broadened to apply in non-international armed conflicts as well.). SEE ALSO Hayley Evans & Natalie Salmanowitz, LETHAL AUTONOMOUS WEAPONS SYSTEMS: RECENT DEVELOPMENTS, Lawfare (Mar. 7, 2019, 3:28 PM), https://www.lawfareblog.com/lethal-autonomous-weapons-systems-recent-developments; Cong. Research Service, Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems 1 (2019), https://fas.org/sgp/crs/natsec/IF11150.pdf; Ashley Deeks, PREDICTING ENEMIES: MILITARY USE OF PREDICTIVE ALGORITHMS, Lawfare (Apr. 10, 2018, 7:00 AM), https://www.lawfareblog.com/predicting-enemies-military-use-predictive-algorithms.

15. According to the Campaign Stop Killer Robots, China delegation to the CCW expressed the wish to ban THE USE of "fully autonomous weapon systems." However, the Chinese government has been investing largely on AWS. Although China questions very much the possibility of AWS complying with the rules of precaution, distinction and proportionality, China already manufacturers the Ziyan Blowfish (unmanned weaponised helicopter with a high level of autonomy) and it expects to deploy in the early 2020s unmanned submarines for mine placement and even suicide attacks against enemy vessels. China, GROUP OF GOVERNMENTAL EXPERTS OF THE HIGH CONTRACTING PARTIES TO THE CONVENTION ON PROHIBITIONS OR RESTRICTIONS ON THE USE OF CERTAIN CONVENTIONAL WEAPONS WHICH MAY BE DEEMED TO BE EXCESSIVELY INJURIOUS OR TO HAVE INDISCRIMINATE EFFECTS. POSITION PAPER SUBMITTED BY CHINA (2018), https://www.unog.ch/80256EDD006B8954/(httpAssets)/E42AE83BDB3525D0C125826C0040B262/$file/CCW_GGE.1_2018_WP.7.pdf (last visited Mar 5, 2018); SEE ALSO Ciarán Daly, IS CHINA'S INTEREST IN AUTONOMOUS WEAPONS CAUSE FOR CONCERN?, AI Business (June 27, 2019), https://aibusiness.com/document.asp?doc_id=760973&site=aibusiness; Elsa Kania, CHINA'S STRATEGIC AMBIGUITY AND SHIFTING APPROACH TO LETHAL AUTONOMOUS WEAPONS SYSTEMS, Lawfare (Apr. 17, 2018, 3:17 PM), https://www.lawfareblog.com/chinas-strategic-ambiguity-and-shifting-approach-lethal-autonomous-weapons-systems#.

16. COUNTRY VIEWS ON KILLER ROBOTS, Campaign to Stop Killer Robots (Oct. 25, 2019), https://www.stopkillerrobots.org/wp-content/uploads/2019/10/KRC_CountryViews_25Oct2019rev.pdf.

that these systems will ever comply with IHL requirements.[17] In contrast, countries such Australia, China, India, Israel, South Korea, the United Kingdom, and the United States are among the States that are already developing autonomous technology, or are otherwise forcefully opposed to any pre-emptive legal regulation of autonomous weapons.[18]

For the purposes of this study, an AWS is defined as: a weapon system designed and programmed for a mission, to be adaptive, and to identify, select, and engage military targets without human intervention.[19] The definition includes three fundamental elements which allow an AWS to be characterised as such. First, AWS should be considered a *weapon system*, rather than a new agent on the battlefield.[20] Therefore, they should not be qualified

17. Hayley Evans, LETHAL AUTONOMOUS WEAPONS SYSTEMS AT THE FIRST AND SECOND U.N. GGE MEETINGS, Lawfare (Apr. 9, 2018, 9:00 AM), https://www.lawfareblog.com/lethal-autonomous-weapons-systems-first-and-second-un-gge-meetings.

18. Damien Gayle, UK, US AND RUSSIA AMONG THOSE OPPOSING KILLER ROBOT BAN, The Guardian (March 29, 2019, 10:25 AM), https://www.theguardian.com/science/2019/mar/29/uk-us-russia-opposing-killer-robot-ban-un-ai; SEE ALSO Alexandra Brzozowski, NO PROGRESS IN UN TALKS ON REGULATING LETHAL AUTONOMOUS WEAPONS, Euractiv (Nov. 22, 2019, updated Dec. 10, 2019), https://www.euractiv.com/section/global-europe/news/no-progress-in-un-talks-on-regulating-lethal-autonomous-weapons/; Ray Acheson, This Cannot Be Kicked Down the Road Any Further, 7 CCW Report 1, 2 (2019), https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2019/gge/reports/CCWR7.6.pdf.

19. Afonso Seixas-Nunes, SJ, THE LEGALITY AND ACCOUNTABILITY FOR AUTONOMOUS WEAPON SYSTEMS. A HUMANITARIAN LAW PERSPECTIVE (Forthcoming 2022). Autonomous Weapons Systems should not be confused with cyber weapons. Although they share some common features, such as their heavy dependence on modern systems of data collection and raise the same level of debate regarding the understanding and future regulation, the distinction adopted here is the one given by the SUMMER STUDY ON AUTONOMY, published by the USA Defence Science Board in June 2016. While cyber-weapons incorporate AUTONOMY AT REST operating virtually as software, whereas AWS incorporate AUTONOMY IN MOTION having a physical presence in the world, such as robots. Department of Defense - Defense Science Board, Summer Study on Autonomy (2016).

20. Brent J. Steele & Eric A. Heinze, FROM SMART TO AUTONOMOUS SYSTEMS: CONFOUNDING TERRITORIALITY AND MORAL AGENCY, IN The Future of Just War: New Critical Essays 98, 99 (Caron E. Gentry &

as some kind of "mitigated reality" which combines the best of machine and human capabilities.[21] Second, in order to step back from idealist, science fiction scenarios, AWS must always be understood to be designed and programmed by human agents.[22] In reality, the intended design, the variables and weights of the program, and the end of a machine learning algorithm will all be established by military personnel. Accordingly, there apparently seems to be no place for independent action or an AWS' "self-determination."[23] Finally, an aspect that roboticists have been reinforcing but which is frequently forgotten by scholars, is that the AWS' algorithms will not be designed for general or uncertain missions, but rather for *well-defined and specific military operations*.[24] Therefore, this article suggests that *the mission* entrusted to a system takes the form of an *algorithm for the mission*, operating according to pre-established human goals. Thus, when it is said that AWS' true novelty is to condemn humans to be *out of the loop,* this can only be said to refer to the moment *after* the system is activated. After activation, the collection and organization of data, the selection of optimal course of action, and the engagement of a target is done by the system without human intervention. Nevertheless, the constraints on the way which the system operates were designed and programmed by human operators. As the US Department of Defense (DoD) has clarified, "human judgment over the use of force does not require manual human 'control' of the weapon system,

---

Amy E. Eckert eds., 2014); SEE ALSO Tim McFarland & Tim McCormack, MIND THE GAP: CAN DEVELOPERS OF AUTONOMOUS WEAPONS SYSTEMS BE LIABLE FOR WAR CRIMES?, 90 Int. L. Stud. 361, 362 (2014).

21. Thompson Chengeta, ARE AUTONOMOUS WEAPON SYSTEMS THE SUBJECT OF ARTICLE 36 OF ADDITIONAL PROTOCOL I TO THE GENEVA CONVENTIONS?, 23 Univ. Cal. Davis j. Int'l L. & Pol'y 65, 75–79 (2016).

22. Simon Chesterman, ARTIFICIAL INTELLIGENCE AND THE PROBLEM OF AUTONOMY, 1 Notre Dame J. Emerging Tech. 210, 232 (2020).

23. Arkin, SUPRA note 10, at 37.

24. *Id*. at 38. (As Ronal Arkin explains, "at the highest level, a human is still in the loop so to speak—commanders must define the mission for the autonomous agent whether it be a human soldier or a robot. The war fighter, robot or human, must then abide by the Rules of Engagement and Laws of War as prescribed from their training or encoding. Autonomy in this sense is limited when compared to a philosopher's point of view.").

as is often reported, but rather broader human involvement in decisions about how, when, where, and why the weapon will be employed."[25]

Considering the above, one might ask why machine-learning algorithms have created such noise amidst States, international organizations, and scholars. Indeed, to understand the full consequences of deploying AWS, it is necessary to revisit fundamental notions of artificial intelligence, particularly concepts known as *deep learning* and *machine learning algorithms*.

A. The Novelty of Machine-Learning Algorithms and its Legal Challenges

The idea of weapon systems operating without human intervention must be taken with a pinch of salt. On the one hand, AWS brings a tremendous spectrum of new opportunity, for human operators will no longer be required to be *on* or *in* the loop of a targeting selection-making process.[26] Several arguments have been advanced by both scholars and States in support of the development of AWS, including the decreased human cost of war, especially in respect of the soldiers physical and psychological health;[27] better situational for ground forces and a faster response to strike back enemy forces; fewer financial costs for States; the increased ability to take faster and more accurate decisions, compared to human capability;[28] stronger

25. Cong. Research Service, SUPRA note 14.

26. Yonah Jeremy Bob, THE FUTURE OF AI IN WARFARE AND COUNTERTERRORISM, The Jerusalem Post (Jan. 25, 2020, 10:30 PM), https://www.jpost.com/Jpost-Tech/The-future-of-AI-in-warfare-and-counterterrorism-615112.

27. Seixas-Nunes, SJ, SUPRA note 19.

28. Philip Alston, LETHAL ROBOTIC TECHNOLOGIES: THE IMPLICATIONS FOR HUMAN RIGHTS AND INTERNATIONAL HUMANITARIAN LAW., 21 J. L., Info. & Sci. 35, 48 (2011); SEE ALSO Christof Heyns, (Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions), REPORT OF THE SPECIAL RAPPORTEUR ON EXTRAJUDICIAL, SUMMARY OR ARBITRARY EXECUTIONS IN MEXICO, U.N. Doc. A/HRC/23/47 (Apr. 28, 2014) 53–54, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-47_en.pdf; SEE ALSO Paul Scharre, Army of None: Autonomous Weapons and the Future of War 13 (2018); 2019 UK Statement. Agenda item 5(a): an exploration of the potential challenges posed by emerging technologies in the area of Lethal Autonomous Weapons Systems to International Humanitarian Law, (2019),

implementation of IHL and greater facility to investigate or report "incidents involving potential violations, enhancing the ability to implement corrective actions, and automatically generating information on unexploded ordnance."[29] On the other hand, advances in AI when introduced to the realm of AWS bring with them the possibility of multiple unintended and unlawful adverse consequences on the ground that require particular attention from the academia today.[30]

---

https://www.unog.ch/80256EDD006B8954/(httpAssets)/1ED3972D40AE53B5C12583D3003F8E5E/$file/20190318-5(a)_IHL_Statement.pdf.

29. Vincent C. Müller, AUTONOMOUS KILLER ROBOTS ARE PROBABLY GOOD NEWS, IN Drones and Responsibility: Legal, Philosophical and Socio-Technical Perspectives on the Use of Remotely Controlled Weapons 67, 69 (Ezio Di Nucci & Filippo Santoni de Sio eds., 2016). [THE PAGINATION APPEARS TO BE OFF FOR THIS SOURCE]. SEE ALSO Tetayana Krupiy, OF SOULS, SPIRITS AND GHOSTS: TRANSPOSING THE APPLICATION OF THE RULES OF TARGETING TO LETHAL AUTONOMOUS ROBOTS, 16 Melb. J. Int'l L. 145, 146–47 (2015); Arkin, SUPRA note 10, at 29–31;

Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, IMPLEMENTING INTERNATIONAL HUMANITARIAN LAW IN THE USE OF AUTONOMY IN WEAPON SYSTEMS, WORKING PAPER, U.N. Doc. CCW/GGE.1/2019/WP.5 (Mar. 28, 2019) https://www.unog.ch/80256EDD006B8954/(httpAssets)/B2A09D0D6083CB7CC125841E0035529D/$file/CCW_GGE.1_2019_WP.5.pdf.; The Russian Federation, 2019 Group of Governmental Experts: Potential Opportunities and Limitations of Military Uses of Lethal Autonomous Weapons Systems ¶ 2 (2019), https://www.unog.ch/80256EDD006B8954/(httpAssets)/B7C992A51A9FC8BFC12583BB00637BB9/$file/CCW.GGE.1.2019.WP.1_R+E.pdf; Scharre, SUPRA note 28, at 302–08; Trevor Phillips-Levine, Dylan Phillips-Levine & Walker Mills, UNMANNED, LETHAL AND ORGANIC: THE FUTURE OF AIR SUPPORT FOR GROUND COMBAT FORCES, Modern War Institute at West Point (Jul. 1, 2020), https://mwi.usma.edu/unmanned-lethal-organic-future-air-support-ground-combat-forces/.

30. Int'l Comm. of the Red Cross (ICRC), International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Recommitting to Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions, 15–37 (2019), https://www.icrc.org/sites/default/files/document/file_list/challenges-report_new-technologies-of-warfare.pdf.

States' armed forces have been using weaponry with limited autonomy for some time now, but only capable of identifying predetermined military targets, but new advances in artificial intelligence allow roboticists to envisage scenarios in which *the mission* entrusted to an AWS can be performed exclusively by the system.[31] Bearing in mind the model developed by John Boyd to explain a human decision-making process—the well-known cycle *observe-orient-decision-action*, or the "OODA Loop"—when applied to AWS would no longer require the presence of a human operator.[32] For example take the Switchblade drone, a weapon weighs less than 3kg and can be carried in a simple back bag.[33] Although the target is preselected by a human operator, this weapon flies autonomously and can provide real-time GPS coordinates, video information, and object recognition.[34] It is not impossible to think that such a system in the future could be entrusted to recognize and target all armed vehicles in a certain area allocated to that system. Under this scenario, the collection and organization of data, identification of possible targets, and their lethal engagement would be delegated to the system. In short, the mission is given to the system, which can then

---

31. Several automatic and semi-autonomous systems are already operating and use by States such Samsung Sentris, Iron Dume, AEGIS and the Brimstone Missile, among others. SEE Arkin, SUPRA note 10, at ch. 2. As Governmental Experts from EU, the UK and the USA have reinforced during the discussions held in Geneva, such systems should not be confused with 'lethal autonomous weapons'. SEE EU STATEMENT ON LAWS, SUPRA note 10; U.K and N. Ir,. Statement, SUPRA note 10; Meier, SUPRA note 10.

32. Frans P. B. Osinga, SCIENCE, STRATEGY AND WAR: THE STRATEGIC THEORY OF JOHN BOYD, IN Series: Strategy and History 2 (Colin Gray & Williamson Murray eds., 2007); SEE ALSO David G. Ullman, "OO-OO-OO!" THE SOUND OF A BROKEN OODA LOOP, J. Def. Software Eng'g 22, 22–25 (2007); Shin-Shin Hua, MACHINE LEARNING WEAPONS AND INTERNATIONAL HUMANITARIAN LAW: RETHINKING MEANINGFUL HUMAN CONTROL, 51 Geo. J. Int'l L. 117, 122–23 (2019); SEE ALSO M. Shane Riza, Killing Without Heart: Limits on Robotic Warfare in an Age of Persistent Conflict 40–41 (2013).

33. Switchblade Drone, AV AeroVironment, https://www.avinc.com/tms/switchblade.

34. David Szondy, SWITCHBLADE 600 DRONE PROVIDES IMPROVED LOITERING MISSILE CAPABILITY, New Atlas (Oct. 5, 2020), https://newatlas.com/military/switchblade-600-loitering-drone/.

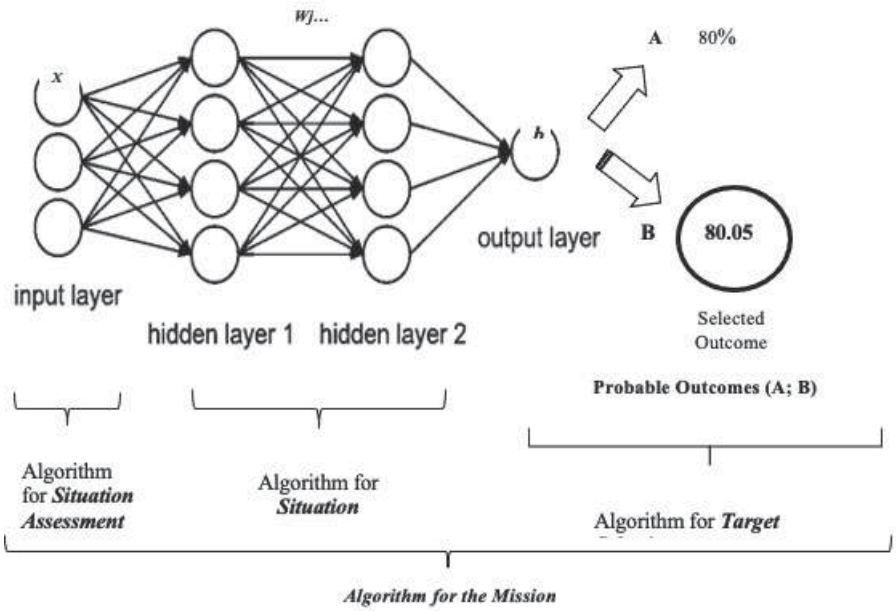
autonomously select a target, including when and how it will be engaged.

In technical computer language, the *mission* would correspond to the *function of a program*. But, in order for a system to execute the mission, its program (P) might demand a sub-set of programs ($_{p1; p2; p3....}$). An *algorithm* is precisely the total sum of those programs, that is, the procedure supporting the execution of the mission.[35] Thus, for example, if an AWS is entrusted with finding and targeting *X*, the *algorithm for the mission* will include all the programs for collecting and processing data, and selecting and targeting the best possible outcome. It might be helpful if the *algorithm for the mission* is thought to display a tri-partite structure, in order to explain the OODA Loop different steps when performed by an AWS. Hence, (1) the *algorithm for situation assessment* collects all relevant data (variables *x*); (2) the *algorithm for situation management* is designed to select the best possible outcome (attending to the different weights $_{w1; w2....}$ and the mutable circumstances of the battlefield); and (3) the *algorithm for target selection* (where weights such as *bias weight (b)* is taken into account).[36]

Figure 1 provides an example of how machine-learning algorithm operates (e.g. a neural network).

35. Noson S. Yanofsky, TOWARDS A DEFINITION OF AN ALGORITHM, 21 J. Log. Comput. 254–55 (2011). (More informally an algorithm can also be defined as a well-defined computational procedure that takes some value, or set of values, as input and produces some value, or set of values, as output.).

[36] The *bias* is a weight. Imagining a *military mission* is being designed and programmed (trying to make a human decision). One has to think about all possible (or observable) factors. But what about parameters that have not come across? What about factors that were not considered? In a Neural Net, there is an attempt to account for these unforeseen or non-observable factors. This is the *bias*. Every neuron that is not on the input layer has a bias attached to it, and the bias, just like the weight, carries a value. Temi Babs, *The Mathematics of Neural Networks*, COINMONKS (2018), https://medium.com/coinmonks/the-mathematics-of-neural-network-60a112dd3e05.



Source: Author

The complexity of machine-learning algorithms, such as the one displayed above, is generally left to roboticists and most of the time disregarded by scholars.[37] However, since the deployment of AWS will inevitably affect the rights of combatants and civilians, and the obligations of the deploying State, some understanding of the technicalities of those systems is required.[38] The highest profile breakthrough in artificial intelligence over the past two decades has come from a subfield of machine learning known as a *deep learning*.[39] Deep learning involves the use of

37. Hua, SUPRA note 32, at 120.

38. Chesterman, SUPRA note 22, at 214.

39. Arlindo Oliveira, The Digital Mind: How Science is Redefining Humanity 107–10 (2017). "Deep learning" refers to the fact that a neural network can have multiple layers (deep) but also that those algorithms can learn. A neural network learns by the acquisition of new supervised or unsupervised data which will allow the neural network to update over time. Deep learning is at the base of most recent AI achievements, such as computer vision language translation and, above all, establishing connections between data unknown to human operators. (see footnote 40). SEE ALSO Max Tegmark, Life 3.0: Being Human in the Age of Artificial Intelligence 101–10 (2017); Stuart J.

artificial neural networks that are inspired by the way in which neurons in the human brain are thought to interact with each other, as shown in Fig 1 ($_{w1;\ wj}$….).[40] *Neural networks* are at the foundation of current military technology and of future AWS.[41] Neural networks are human-designed, goal-oriented algorithms which can be designed through a process of trial and error dubbed *reinforcement learning* (RL) optimising the best *probable* result.[42] They are able to establish not causal but *predictive patterns* between the data given to the system and, based in probabilities, to identify accurately military targets.[43] Any modality of

---

Russell & Peter Norvig, Artificial Intelligence: A Modern Approach, 693–96 (3rd ed. 2010).

40. Daniel Nelson, WHAT IS DEEP LEARNING?, UNITE.AI (last updated Nov. 28, 2020), https://www.unite.ai/what-is-deep-learning/; SEE ALSO Gregor Noll, WAR BY ALGORITHM: THE END OF LAW?, IN War and Algorithm 75, 80 (Max Liljefors, Gregor Noll, & Daniel Steuer eds., 2019); Krupiy, SUPRA note 29, at 199; Stuart Russell, Human Compatible: Artificial Intelligence and the Problem of Control 171–72, 295–96 (2019); Tetyana Krupiy, REGULATING A GAME CHANGER: USING A DISTRIBUTED APPROACH TO DEVELOP AN ACCOUNTABILITY FRAMEWORK FOR LETHAL AUTONOMOUS WEAPON SYSTEMS, 50 Geo. J. Int'l L. 45, 75–76 (2018).

41. George Leopold, U.S. MILITARY DEPLOYS NEURAL NETWORK TECHNOLOGY, EE Times (Jul. 17, 2001), https://www.eetimes.com/u-s-military-deploys-neural-network-technology/#; SEE ALSO Frank Wolfe, FLEXIBLE NEURAL NETWORKS NEEDED FOR FCAS, AIRBUS OFFICIAL SAYS, Aviation today (May 19, 2020), https://www.aviationtoday.com/2020/05/19/flexible-neural-networks-needed-fcas-airbus-official-says/.

42 Linell A. Letendre, *Lethal Autonomous Weapon Systems: Translating Geek Speak for Lawyers*, 96 INT. LAW STUD. 274–294, 290–291 (2020). A GUIDE TO USING ARTIFICIAL INTELLIGENCE IN THE PUBLIC SECTOR, 1–48 11 (2020), https://www.gov.uk/government/publications/a-guide-to-using-artificial-intelligence-in-the-public-sector (last visited Mar 3, 2021).

43. SEE Sally Cole, EXPLAINABLE INTELLIGENCE IS ON THE WAY FOR NEURAL NETWORKS, Military Embedded Systems (June 10, 2019), http://mil-embedded.com/articles/explainable-intelligence-is-on-the-way-for-neural-networks/. On this regard it is important to distinguish SUPERVISED LEARNING ALGORITHMS from UNSUPERVISED LEARNING ALGORITHMS. In supervised learning, the training data is labelled by human operators, while in unsupervised learning the algorithm proceeds by looking for patterns in unlabelled data periods in general. The most applied model is supervised learning algorithms specially developed for target recognition. The system is trained, for

"deep learning" can bring advantages to the battlefield: the system can "learn" while performing the entrusted mission, *adapting the system to environmental uncertainties without requiring human input*.[44] However, according to AI experts "systems that are based on RL have significantly higher risks of causing major damages in the real-world compared to other machine learning methods such as classification."[45] Autonomous technology opens a Pandora's Box with its inherent unpredictability. In other words, it is possible to say that unpredictability results from the impossibility of predicting how new inputs will be processed in the different layers, and also because it is highly questionable whether the *why* and *how* of a selection-making process outcome will ever be accessible to human understanding.[46] The reasons explain why autonomous systems have been baptized *black-box systems*: systems whose workings are opaque to its human operators or to military commanders, i.e. the *inputs* and *outputs* are observable but the processes that take place between, that is, the structural interrelations amongst the data, are invisible.[47]

---

example to identify a weapon, by presenting to the system images of weapons hundreds of billions of times. Then the system when handling with data or translating the pixels organises all according to the right format learned by the system. SEE ALSO PREDICTING CIVIL CONFLICT: WHAT CAN MACHINE LEARNING TELL US? Vision of Humanity, http://visionofhumanity.org/economists-on-peace/predicting-civil-conflict-can-machine-learning-tell-us/ (last visited May 20, 2020); Hua, SUPRA note 32, at 124.

44. Daniel Nelson, WHAT IS DEEP REINFORCEMENT LEARNING?, UNITE.AI (Oct. 13, 2019, last updated Aug. 2, 2021), https://www.unite.ai/what-is-deep-reinforcement-learning/; SEE ALSO Hua, SUPRA note 32, at 124–25; ICRC, SUPRA note 30, at 31; Kenneth Anderson & Matthew C. Waxman, DEBATING AUTONOMOUS WEAPON SYSTEMS, THEIR ETHICS, AND THEIR REGULATION UNDER INTERNATIONAL LAW, IN The Oxford Handbook of L., Regul., & Tech. 1097, 1100–03 (Roger Brownsword, Eloise Scotford, & Karen Yeung eds., 2017); Krupiy, SUPRA note 40, at 75–78.

45. Antoine Tardif, VAHID BEHZADAN, DIRECTOR OF SECURED AND ASSURED INTELLIGENT LEARNING (SAIL) LAB – INTERVIEW SERIES, UNITE.AI (Apr. 27, 2020), https://www.unite.ai/vahid-behzadan-director-of-secured-and-assured-intelligent-learning-sail-lab-interview-series/.

46. Hua, SUPRA note 32, at 119.

47. Noll, SUPRA note 40, at 83.

Traditionally, a weapon system would rely on pre-determined algorithms which are "very detailed recipes-sequences of small steps a computer executes to obtain some specific result."[48] Systems could be said to be *reliable*. Weapon systems would be an extension of human soldiers on the battlefield, reproducing human orders. However, with the advent of machine-learning algorithms, systems "learn" from the ground, collect new data with a velocity, variety, and volume that would be nearly impossible for any human operator.[49] From the collected data (*algorithm for situation assessment*), the *algorithm for situation management* can establish what data features to choose, what conditions to use to allow an AWS to select the best course of action possible, and engage the target (*algorithm for target selection*) without human intervention.[50]

The *algorithm for the situation assessment* is particularly important when it is taken into account that AWS algorithms must

48. Oliveira, SUPRA note 39, at 6–7.

49. Int'l Comm. of the Red Cross (ICRC), Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach, (2019) https://www.icrc.org/en/download/file/96992/ai_and_machine_learning_in_armed_conflict-icrc.pdf.

50. At this point it is important to distinguish automated from autonomous systems. Many systems have already automated functions which process is pre-established, and a human operator can always supervise (e.g. cruise control of a plane). With autonomous systems means that the system operates without possible intervention of its initial human operators (e.g. programmers; military commanders), except the activation/deactivation of the system. SEE Chesterman, SUPRA note 22, at 212. SEE ALSO Matthew U. Scherer, Allan G. King & Marko N. Mrkonich, APPLYING OLD RULES TO NEW TOOLS: EMPLOYMENT DISCRIMINATION LAW IN THE AGE OF ALGORITHMS, 71 S. C. L. Rev. 2, 3–5 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3472805&download=yes; Cong. Research Service, SUPRA note 14; ICRC, SUPRA note 30, at 31 (as an example of confusion between the different terms); UK Ministry of Defence, The UK Approach to Unmanned Aircraft Systems, Joint Doctrine Note 2/11 (Mar. 30, 2011), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644084/20110505-JDN_2-11_UAS_archived-U.pdf. The document states that "not all autonomous weapon systems incorporates AI." Autonomy should be taken as the technical capability of a system to replicate human decision-making processes, and not as a repetitive mechanism of deterministic tasks. This distinction was at the center of the first policy document published by the UK.

be able *to adapt* the system to new circumstances on the battlefield in order to ensure that the selection algorithm engages the accurate military targets.[51] This element explains why AWS must depend upon embedded machine-learning algorithms which, by definition, are not *deterministic* but *unpredictable algorithms,* for two sets of reasons.[52] First, the algorithms need to be *open algorithms* to the environment and collect new relevant data and adapt the *algorithm for the mission*.[53] As roboticists underline, a problem with adaptive algorithms is the need to control the data the system acquires after being activated, and how to prevent the algorithms from creating bias.[54] Second, machine-learning algorithms select and engage military targets based on probabilities.[55] The outcome chosen will be the most the probable of the sets of possibilities in order to obtain the best possible outcome. As it was possible to observe in Fig. 1, it is not the result of a set of human discerned reasons, but rather that of the system's "reasons" and a human qualitative judgment that gives place to a quantifiable choice. In the eventuality of AWS causing unlawful actions on the battlefield, the major concern to roboticists—and also to lawyers—will be to explain and understand what happens within the system's black box.[56] While

---

51. Hua, SUPRA note 32, at 119; SEE ALSO Noel Sharkey, STAYING IN THE LOOP: HUMAN SUPERVISORY CONTROL OF WEAPONS, IN Autonomous Weapons Systems. L., Ethics, Pol'y 23–38, 48–51 (Nehal Bhuta, Susanne Beck, Robin Geiß, Hin-Yan Liu & Claus Kreß eds., 2016); Sassoli, SUPRA note 5, at 10.73 (517).

52. Krupiy, SUPRA note 29, at 149–50; SEE ALSO ICRC SUPRA note 30, at 31–32.

53. Nick Bostrom, SuperIntelligence: Paths, Dangers, Strategies 155–76 (2014).

54. Prashant Gupta, DECISION TREES IN MACHINE LEARNING, Towards Data Science (May 17, 2017), https://towardsdatascience.com/decision-trees-in-machine-learning-641b9c4e8052; SEE GENERALLY U.N. Inst. for Disarmament Resarch (UNIDIR), Algorithmic Bias and the Weaponization of Increasingly Autonomous Technologies 1–18 (2018).

55. Pedro Domingos, The Master Algorithm - How to Quest for the Ultimate learning Machine will Remake Our World. 153–75 (2015); SEE ALSO Russell & Norvig, SUPRA note 39, at 285–95.

56. SEE Frank Pasquale, The Black Box Society: The Secret Algorithms that Control Money and Information 3 (2015) (A "Black-Box System" is a system whose workings are carried out without monitoring by its human operators or military commanders', i.e. the INPUTS

roboticists will focus on how this result could have happened, lawyers will be rather concerned with who will be responsible.

B. Problematic Scenarios of Machine-Learning Algorithms: "Errors" of the System and Problems of Accountability

Bearing in mind possible violations of IHL caused by AWS, it is possible to specify four likely causes: criminal use of the system; poor design; malfunctions and errors. The first two causes concern mainly individual criminal responsibility, which go far beyond the aim of this work. Malfunctions and errors, on the other hand, depend more on how the deploying State complies with its obligation to prevent IHL violations. These obligations are a priori because States must ensure that those systems are apt to perform according to the intention for which they were designed, respecting at the same time the rules of IHL.

For decades, algorithms have been used in military technology, but never before has a selection-making process been entrusted to a weapon system. This raises concerns about how *direct human control* is indispensable during the OODA Loop stages.[57] In the words of the United States DoD, human control means that "a human determination that the weapon will be used 'with appropriate care and in accordance with the law of war, applicable treaties, weapon system safety rules, and applicable rules of engagement,'" but *before* the weapon is activated.[58] But once the system is activated, human operators will no longer have access to the *algorithm for situation management*.[59] Thus,

---

and OUTPUTS are observable but the processes that take place between (the structural interrelations amongst the data) are invisible.). SEE ALSO Simon Chesterman, THROUGH A GLASS, DARKLY: ARTIFICIAL INTELLIGENCE AND THE PROBLEM OF OPACITY, Am. J. Compar. L. (forthcoming 2021).

57. SEE GENERALLY Governments statements from Brazil, Costa Rica, Germany, Greece, Holy See, Netherlands, Pakistan, Turkey, the United Kingdom, South Africa, Sri Lanka, Sweden, among others. See 2016; 2017; 2018 and 2019 Group of Governmental Experts on LAWS available at https://www.unog.ch/80256EE600585943/(httpPages)/37D51189AC4FB6E1C1257F4D004CAFB2?OpenDocument

58. Cong. Research Service, SUPRA note 14 (emphasis added).

59. SEE Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be

the way data will be processed by an AWS is hidden from human operators, and the system will operate according to the constraints designed a priori.[60] Several States and authors take issue with such a type of human control, asking whether an exclusively *a priori human control* will ever be enough.[61]

There is no doubt that the increasing capacity and reliability of computers has considerably changed the role of human operators.[62] However, it must be said that phenomena such as "lack of human control" and "automation bias" are not excluded from deterministic and automated systems.[63] Regarding the former,

---

Excessively Injurious or to Have Indiscriminate Effects, U.N. Doc. CCW/GGE.1/2017/WP.2 (October 9, 2017), http://undocs.org/ccw/gge.1/2017/WP.2. (The definition of AWS presented by the Netherlands highlights precisely the element of impossibility of human intervention once the system is activated, by stating that s AWS is "weapon that, without human intervention, selects and engages targets matching certain predefined criteria, following a human decision to deploy the weapon on the understanding that an attack, once launched, cannot be stopped by human intervention.").

60. Tim McFarland, Autonomous Weapon Systems and the Law of Armed Conflict: Compatibility with International Humanitarian Law 40 (2020).

61. Krupiy, SUPRA note 29, at 155–56; SEE ALSO Hua, SUPRA note 32, at 126. (According to Shin-Shin Hua this sort of control would violate IHL rules as the principle of precaution that demand "constant care" to comply with the principle of distinction and proportionality.). SEE ALSO Christof Heyns, AUTONOMOUS WEAPONS IN ARMED CONFLICT AND THE RIGHT TO A DIGNIFIED LIFE: AN AFRICAN PERSPECTIVE, 33 S. Afr. J. Hum. Rights 46, 67 (2017); Daniele Amoroso & Guglielmo Tamburrini, Int'l. Comm. for Robot Arms Control, What Makes Human Control over Weapon Systems "Meaningful"? 3–6 (2019), https://www.icrac.net/wp-content/uploads/2019/08/Amoroso-Tamburrini_Human-Control_ICRAC-WP4.pdf.

62. McFarland, SUPRA note 59, at 48.

63. Ashley Deeks, Noam Lubell & Daragh Murray, MACHINE LEARNING, ARTIFICIAL INTELLIGENCE, AND THE USE OF FORCE BY STATES, 10 J. Natl. Sec. L. Pol'y 1, 17–18 (2019); SEE ALSO Noll, SUPRA note 40, at 88; Peter Asaro, ON BANNING AUTONOMOUS WEAPON SYSTEMS: HUMAN RIGHTS, AUTOMATION AND THE DEHUMANIZATION OF LETHAL DECISION-MAKING, 94 Int'l. Rev. Red Cross 687, 699–701 (2012). (Some authors, such as Peter Asaro, believe that in the absence of human judgement it is impossible to ensure that the killing is not arbitrary, since "human judgment is constitutive of the system of justice." However, these authors tend to neglect the problems of

human control is always present before a weapon is deployed on the battlefield; but it must be acknowledged that when a munition is launched, there is very little that a human operator can do.[64] Turning to the latter, progress in computer science has led humans take a more passive role as supervisors of automated processes, which leaves open the risk of operator's error by means of uncritical confirmation of systems' estimates without the requisite cross-checking of information; i.e., the phenomenon known as *automation bias*.[65] It is indeed a double-edged problem. On one hand, States and scholars insist on the importance of human control; on the other, when it is possible to exercise human control, operators tend to trust in "unquestionable" predictions. When the complexity of the modern battlefield is taken into consideration, it is not apparent how human control can be guaranteed in every step of the decision-making process.

Looking at a more technical side, hardware and technical failures happen, sometimes causing civilian damage (e.g. a bomb is released without human permission because the lock system fails). In short, malfunctions inevitably occur in spite of humans being *in the loop*, and cannot necessarily be attributed to any human fault.

Conversely, looking at Fig 1, machine-learning algorithms can commit "errors" in multiple ways throughout the selection-making process.[66] In this type of scenario, it is at the system's software level that an "error" caused IHL violations. In cases where the AWS fails to accurately interpret the properties of the environment in which it is deployed conducting erroneous selection-making process, the unlawful unpredictable outcomes which are produced by an AWS should be termed "syntax-errors" or simply "errors." When an error occurs, an AWS co-authors itself

---

"automation bias," and how it is almost humanely impossible to process all the information that weapons system have of the battlefield.).

64. Deeks, Lubell, & Murray, SUPRA note 62, at 16.

65. J. Elin Bahner, Anke-Dorothea Hüper & Dietrich Manzey, MISUSE OF AUTOMATED DECISION AIDS: COMPLACENCY, AUTOMATION BIAS AND THE IMPACT OF TRAINING EXPERIENCE, 66 Int'l. J. Hum.-Comput. Stud. 688, 689; SEE ALSO Lorna McGregor, Daragh Murray & Vivian Ng, INTERNATIONAL HUMAN RIGHTS LAW AS A FRAMEWORK FOR ALGORITHMIC ACCOUNTABILITY, 68 Int'l. Comp. L. Q. 309, 317–18 (2019).

66. McFarland, SUPRA note 59, at 60.

through its learning capacity, deviating from the pre-established human goal, and demonstrating that it possesses an "original normativity" that can only be traced back to the system and not to any human operator.[67] This solution presents the only way of taking seriously the implications of MAL embedded within AWS. Calling to mind the model present in Figure 1, it is not difficult to imagine a system that develops *data bias*; ponders incorrectly the different weights; or, finally, opts for the most probable, best outcome, which is ultimately revealed to be contrary to IHL. The immediate question to ask is: Who should be held accountable in the situations of errors?

Thomas W. Simpson and Vincent Muller suggest an important and perceptive moral reading of the AWS' accountability problems. These authors introduce the concept of "engineering

67. The problem has become a subject of attention for the jurisprudence of the USA and the UK, where courts still refuse to recognise authorship to those other than humans. AI CANNOT BE RECOGNISED AS AN INVENTOR, US RULES, BBC News Technology (Apr. 29, 2020), https://www.bbc.co.uk/news/technology-52474250. SEE ALSO Krupiy, SUPRA note 29, at 185. T. Krupiy, recognised several differences between "human error" and "machine error'" when analysing an incident involving Israeli technology in 2006. However, Professor Krupiy understands that one of the differences between "human error" and "machine error" is that in a situation of a conventional weapon, "individuals plan an attack that complies with the rules of targeting, but the weapon fails to explode, whereas when it comes to LARs, the malfunction which leads to civilians being killed OCCURS BEFORE THE ROBOT LAUNCHES AN ATTACK, BUT AFTER A HUMAN DECISION-MAKER MADE THE DECISION TO SEND THE ROBOT ON A MISSION." This understanding begs, nonetheless, some observations. First, for Professor Krupiy a machine error is always a human error, and therefore there is not the possibility of a machine making error caused by the system´s software. However, at the same time Professor Krupiy asks for a thorough analysis of the rate of reliability of AWS; If errors will be always caused by human decision, there would be no need to ask for AWS´s reliability. Second, the situation described as a "machine error" is indeed of criminal nature. Nonetheless, if there is a human decision to deploy a system knowing that the system is defective raises questions of MEN REA and criminal responsibility (Article 25 and 30 of the Rome Statute. SEE ALSO BBC News Technology, SUPRA note 66. (The problem has become a subject of attention for the jurisprudence of the USA and the UK, where courts still refuse to recognise authorship to those other than humans.).

tolerance."[68] They propose that any military system is required to show "sufficient robustness"; that is, there is a "degree of reliability it must meet."[69] Reliable "engineering tolerance" refers to the balance which must be established between the financial costs of any weapon and the advantages it provides, but also factors in the costs for its potential failure.[70] Therefore, there are always certain risks involved in the deployment of any military system.[71] Nonetheless, the authors go beyond this sphere. They conceptualize unforeseeable events occurring "outside the tolerance level" for which no one should be held accountable because they fall into the category of a "permissible malfunction blameworthiness gap."[72] Examples are provided: a bridge that collapses due to extraordinary events;[73] unintended side-effects of some drugs;[74] or parents when they are called upon to be responsible for actions of their children.[75] Responsibility in these cases derives from a moral, and also legal, "duty of care."[76]

In the case of an armed conflict, however, the authors postulate that "tolerance levels should be strict . . ." because civilians would have not given their consent to the hostilities nor to the weapons deployed, and there are no infallible systems.[77] In light of this reasoning, it is possible to hold that "malfunctions" do happen and that they give rise to a "permissible malfunction blameworthiness gap" because they happen within the threshold of a given "engineering tolerance." However, as the authors explain, the deployment of AWS on the battlefield demands serious

68. Müller, SUPRA note 29, at 74–75; SEE ALSO Thomas W. Simpson & Vincent C. Müller, JUST WAR AND ROBOT'S KILLINGS, 66 Phil. Q. 302, 308 (2016).

69. Simpson & Muller, SUPRA note 67, at 307.

70. *Id.*

71. Müller, SUPRA note 29, at 75.

72. Simpson & Muller, SUPRA note 67, at 312.

73. *Id.* at 307.

74. *Id.* at 309.

75. *Id.* at 305.

76. Müller, SUPRA note 29, at 75–77; SEE ALSO Simpson & Muller SUPRA note 67, at 311.

77. Simpson & Muller, SUPRA note 67, at 312.

regulation and "strict tolerance."[78] Mutatis mutandis, a situation involving error calls for some form of liability. First, because errors cannot be considered within the category of engineering tolerance, and, second, an error does result from a violation of a duty of care. The system, its *software,* makes a syntactical error in the way it interprets the world. Indeed, as Nick Bostrom, argues "AI is strong enough that human opposition is ineffectual."[79]

History provides a good number of examples to consider, including the Petrov Case[80] and Iran Flight 655,[81] among others.[82] Two more recent examples are of particular interest. First, the 2019 two accidents involving the Boeing 737 Max model,[83] and

78. *Id*. at 320; SEE ALSO Müller, SUPRA note 29, at 77–78.

79. Bostrom, SUPRA note 52 at 144–45.

80. *Id*. at ch. 10, n.12. The Petrov Case refers to a situation that occurred in September 1983, when the Soviet Oko nuclear early-warning system malfunctioned and reported an incoming US missile strike launched from Montana. The system's mistake was correctly identified by the duty officer at the command centre, Deputy Chief for Combat Algorithms Stanislav Petrov, avoiding what could have instigated World War III.

81. David Akerson, THE ILLEGALITY OF OFFENSIVE LETHAL AUTONOMY, International Humanitarian Law and the Changing Technology of War [NEED CORRECT PAGE] (Dan Saxon ed., 2013). (The IRAN FLIGHT 655 CASE refers to an Iranian flight, which, in July 1988, took off from Bandar Abbas Airport towards Dubai when the United States guided missile cruiser Vincennes fired two missiles at the plane. The US Aegis system was not able to monitor civilian radio channels and detected flight 655 as an Iranian Air Force f-14, a military aircraft, killing 290 civilians on board.).

82. Paul Scharre, Autonomous Weapons and Operational Risk, Ethical Autonomy Project, 29–30 (2016), https://www.cnas.org/publications/reports/autonomous-weapons-and-operational-risk.

83. SEE BOEING 737 MAX LION AIR CRASH CAUSED BY SERIES OF FAILURES, BBC News Business (Oct. 25, 2019), https://www.bbc.co.uk/news/business-50177788. The 737 Max Boeing accidents include the Lion Air Flight 610, which crashed in October 2018 just minutes after taking off from Jakarta, Indonesia, killing 189 people. In March 2020, another Max, Ethiopian Airlines Flight 302, crashed minutes after take-off; all 157 people on board died. In both accidents black box data from the two crashes showed that a system designed to help the plane avoid stalls appears to have malfunctioned, contributing to the accidents.

second, the recent incident caused by the Iranian frigate *Jamaran* when testing a new anti-ship missile.[84] Regarding the Iranian frigate incident, experts tend to offer one of two explanations: either it was a targeting mistake made by the crew, or, more relevantly for our analysis, "Iranian armed forces have a systemic problem with coordination and command and control, whether it's air defense or naval warfare, whether it's the Revolutionary Guards or the army."[85] As to the Boeing example, there is a complex chain of events behind the accidents involving the 737 Max.[86] One element, however, is particularly important: the *Maneuvering Characteristics Augmentation System* (MCAS) used on the 737 Max. This software, which was designed to automatically prevent the 737 Max model from stalling, repeatedly pushed the plane's nose down in both accidents, leaving pilots fighting in vain to regain control of the plane.[87]

The Boeing example is also helpful to distinguish malfunctions from errors. The new 737 Max model is equipped with just one angle of attack (AOA) sensor that provides supplementary

84. Patrick Wintour, IRAN SAYS 19 DEAD IN GULF OF OMAN FRIENDLY FIRE INCIDENT, The Guardian (May 11, 2020, 8:46 AM) https://www.theguardian.com/world/2020/may/11/iranian-navy-ship-hit-by-missile-in-fatal-friendly-fire-incident-in-gulf. The Iranian frigate JAMARAN refers to an accident occurred in May 2020 when, during a military exercise, the Iranian JAMARAN shot and sank another Iranian Navy vessel, the KONARAK by accident and killed about 40 of its personnel on board. The KONARAK was reportedly tasked with placing targets within the firing zone. By the time the JAMARAN fired a cruise missile, however, the KONARAK had not distanced itself enough from the designated target, so the missile locked on it instead. SEE ALSO Farnaz Fassihi, IRANIAN FRIENDLY FIRE KILLS 19 IN 2ND MISSILE ACCIDENT OF YEAR, N.Y. Times (May 10, 2020), https://www.nytimes.com/2020/05/10/world/middleeast/iran-ship-dead.html.

85. Fassihi, SUPRA note 83.

86. Woodrow Bellamy III, LION AIR 737 MAX FINAL ACCIDENT REPORT CITES AOA SENSOR, MCAS AMONG MULTITUDE OF CONTRIBUTING FACTORS, Avionics Int'l (Oct. 28, 2019), https://www.aviationtoday.com/2019/10/28/lion-air-737-max-final-accident-report-cites-aoa-sensor-mcas-as-contributing-factors/.

87. BBC News Business, SUPRA note 82; SEE ALSO John Markoff, A CASE FOR COOPERATION BETWEEN MACHINES AND HUMAN, N.Y. Times (May 21, 2020), https://www.nytimes.com/2020/05/21/technology/ben-shneiderman-automation-humans.html.

information to the flight crew.[88] In both situations, the AOA fed faulty information to the flight control computer, sending the planes into irrecoverable nose-dives, and prevented the pilots from regaining control. This was due to a fault in the AOA sensor that had been damaged by a bird strike, and then improperly repaired by a U.S.-based maintenance repair facility.[89] The fault arising in the AOA sensor may be immediately recognized as a malfunction. However, the system did not simply malfunction, it also erred: firstly, by not identifying data that would lead to inexorably to the destruction of the plane, but also by not allowing humans to regain control of it in spite of the efforts made by the pilots. This example illustrates that when errors occur, there is an inversion of the mission given to the system. In short, the system becomes "independent," preventing human intervention and creating the possibility of an unlawful, unpredictable outcome. By contrast, when malfunction occurs, the situation is the opposite; it would not happen if the human operator had foreseen any hardware problem.

Another case worth mentioning, although for different reasons, is the tragic *human error* that resulted in Malaysian Airlines Flight MH17 being shot down in July 2014.[90] Recently the

---

88. SEE BOEING 737 MAX SOFTWARE UPDATE, Boeing Commercial, https://www.boeing.com/commercial/737max/737-max-software-updates.page. Angle of Attack (AOA) – the difference between the pitch angle (nose direction) of the airplane and the angle of the oncoming wind. The higher and more forward position of 737 Max engines could cause the plane's nose to go up which is a potential danger. The risk would be, however, detected by the AOA that aligns itself with the airstream and the plain's computers would then automatically move the back stabilizers up bringing the plane's nose back down. The 737 Max Model reduce the two existing AOA for only one sensor without any other safeguard.; SEE ALSO Jon Ostrower, WHAT IS THE BOEING 737 MAX MANEUVERING CHARACTERISTICS AUGMENTATION SYSTEM?, The Air Current (Nov. 13, 2018), https://theaircurrent.com/aviation-safety/what-is-the-boeing-737-max-maneuvering-characteristics-augmentation-system-mcas-jt610/.

89. Jack Nicas, Natalie Kitroeff, David Gelles & James Glanz, BOEING BUILT DEADLY ASSUMPTIONS INTO 737 MAX, BLIND TO A LATE DESIGN CHANGE, N.Y. Times (June 1, 2019), https://www.nytimes.com/2019/06/01/business/boeing-737-max-crash.html?auth=login-google; SEE ALSO Bellamy III, SUPRA note 85.

90. SEE GENERALLY German Lopez, THE MH17 PLANE CRASH IN 2014, EXPLAINED, Vox (June 1, 2015, 3:23 PM),

Dutch prosecutor decided to formally charge four fighters of the Dontesk People's Republic (DPR) of crimes committed under the Dutch criminal Law for the destruction of MH17.[91] In their opening statement, the Dutch Public Prosecutor ventilated an important point by arguing that

> it is perfectly conceivable that the true intention of these defendants was to shoot down an aircraft of the Ukrainian armed forces [and not Flight MH17 . . . .] When drawing up the indictment we explicitly took account of this error scenario[; however,] *any error concerning the target makes no difference in respect of the proof that such offences were committed*. That is why, in the Netherlands and in many other countries, people are convicted of murder if they happen to shoot dead a passer-by instead of their intended victim.[92]

In this case the error was human because Flight MH17 was mistaken for a military target by the those in command. Nonetheless, this case asks the question of whether the legal consequences were the same if the plane was shot down by an AWS selection-making process error.

In light of the above, it is, therefore, imperative to distinguish between malfunctions and errors since neither involves human fault. First, malfunctions are associated with hardware, and errors are associated with software. Software is to some extent independent of hardware. While software applies to the algorithms, concepts, and mathematical architecture, hardware applies to the material and structures that allow the system to operate in the external world. Simply put, hardware detects the

---

https://www.vox.com/2014/9/26/18080548/mh17-ukraine-malaysia-airlines.

91. GOVERNMENT INFORMS UN SECURITY COUNCIL ON MH17 TRIAL, Gov't of the Neth. (June 6, 2020, 5:01 PM), https://www.government.nl/latest/news/2020/03/06/government-informs-un-security-council-on-mh17-trial; SEE ALSO Netherlands Public Prosecutor, Opening Statement of the MH17 Trial before the Full-Bench Chamber of The Hague District Court, (Mar. 9, 2020), https://www.prosecutionservice.nl/topics/mh17-plane-crash/prosecution-and-trial/court-sessions-march-2020/opening-statement-9-march-2020 [hereinafter Opening Statement MH17].

92. Opening Statement MH17, SUPRA note 90, at Prosecution Decisions: The Charges (emphasis added).

environment while software makes sense of it. Second, malfunction prevents or interrupts a mission from being accomplished even if it causes violations of IHL, whereas errors lead the system to invert the original predetermined mission and produce a non-programmed outcome chosen by the system. Third, in terms of accountability, the two situations demand different answers. Malfunctions are unforeseeable, while errors should be reasonably foreseen when the system is tested and evaluated, because it concerns the "reasoning" mechanism, or neural networks, of the weapon system.

This last proposition became clear during the investigations of the accidents involving the 737 Max. In January 2016, Ed Wilson, the chief test pilot for the Max, declared that "the 737 Max just felt right in the flight, giving us complete confidence that this airplane will meet our customers' expectations."[93] However, when some changes were subsequently introduced, the Federal Aviation Administration (FAA) was found to have made decisions based on an incomplete assessment of the system: it never tested a malfunctioning sensor and the capacity of the system to adapt to the new circumstances.[94]

It is true that the 737 Max case did not occur in the context of an armed conflict and that it was not also an autonomous system, but it is provocation enough for the mind of any scholar. It is also true that it is difficult for a lawyer to conclusively determine the merits of these claims but, given what is already known about machine-learning algorithms, the risks inherent within military autonomous systems are widely apparent and cannot be underestimated. As Vahid Behzadan, director of the Secured and Assured Intelligent Learning (SAIL) Lab, argues "considering the fundamental susceptibility of current machine learning technologies to *mistakes* and adversarial attacks, I am deeply concerned about the safety and security of even semi-autonomous vehicles . . . . [O]ne of the main problems with AI-enabled weaponry is in the difficulty of controlling the underlying technology."[95] This is because AWS will select and engage military targets based on probabilities in the unpredictable context of the battlefield. Added to this, it must be kept in mind that the

93. Nicas, Kitroeff, Gelles & Glanz, SUPRA note 88.

94. *Id.*; SEE ALSO McFarland, SUPRA note 59, at 38–39.

95. Tardif, SUPRA note 44 (emphasis added).

algorithm for the mission operates inside a black box, so human intervention is impossible before and after the target is engaged, consequentially elevating the level of risk inherent to AWS.

In light of the above, it is possible to draw several conclusions. First, AWS are themselves inherently vulnerable and unpredictable systems. Second, these systems are prone to cause violations of IHL due to system errors, which is a distinctive element of MLA. An error ought to be distinguished from the situations of a malfunction because the respective forms of liability are necessarily different. If a malfunction is a technical failure and no one is to be held accountable under international law, errors, by contrast, are inherent to AWS' risky nature, due to their unpredictability or propensity for syntax errors when they attempt to adapt to new circumstances.[96] Thus, the deploying State must bear the responsibility for the IHL violations caused by AWS. Finally, to consider malfunctions as errors would necessarily lead to a decriminalization and dilution of IHL.

The category of error certainly raises enormous difficulties, starting with evidence and the burden of proof, but ignoring those difficulties would, in effect, lead to the dilution of IHL or give rise to an *accountability gap*. As Norway has argued, "it is easy to foresee situations in which no one can be held responsible if fully autonomous weapons are used in violation of international law.

This potential accountability gap can have very serious consequences and erode the substantial progress that has been achieved in this area over the last few years."[97] However, such a scenario should be treated as more than just an accountability gap, but rather, as an *accountability trap* for considering errors

96. Seixas-Nunes, SJ, SUPRA note 19, at ch. 5; SEE ALSO Ian Henderson, Patrick Keane & Josh Liddy, REMOTE AND AUTONOMOUS WARFARE SYSTEMS: PRECAUTIONS IN ATTACK AND INDIVIDUAL ACCOUNTABILITY, IN Research Handbook on Remote Warfare 335, 361 (Jens David Ohlin ed., 2016).

97. Norway, 2017 GROUP OF GOVERNMENTAL EXPERTS OF THE HIGH CONTRACTING PARTIES TO THE CONVENTION ON PROHIBITIONS OR RESTRICTIONS ON THE USE OF CERTAIN CONVENTIONAL WEAPONS WHICH MAY BE DEEMED TO BE EXCESSIVELY INJURIOUS OR TO HAVE INDISCRIMINATE EFFECTS (2017), https://www.unog.ch/80256EDD006B8954/(httpAssets)/DF861D82B90F3BF4C125823B00413F73/$file/2017_GGE+LAWS_Statement_Norway.pdf.

as malfunctions or a "permissible malfunction blameworthiness gap".[98] These aspects will be developed later in this study, but if errors are not individualized in their specificity, one might ask: What would be the *legal* incentives of any State to "respect" or "ensure respect" (Common Article 1) for the compliance with IHL?

These difficulties cannot be countenanced as a dead-end creating an accountability gap. The nature of State responsibility is predicated on objective liability, and it is not contingent upon the existence of fault or negligent behavior.[99] Thus, the sole existence of conduct attributable to the State contrary to primary norms of International Law is the essence of State responsibility.[100]

One question remains unanswered: Where is the legal support for State responsibility for IHL violations caused by AWS errors to be found? Part 2 examines, first, how to attribute such violations to the deploying State and, second, what obligations of the State are violated in case of errors of AWS.

II. INTERNATIONAL LAW, AWS AND THE OBLIGATIONS OF THE DEPLOYING STATE.

The rules concerning the use for force between States, *jus ad bellum*, are largely enshrined in the United Nations Charter (UN Charter), and one of the most fundamental aims of the UN

---

98. Simpson & Muller, SUPRA note 67, at 312.

99. Riccardo Pisillo-Mazzeschi, THE DUE DILIGENCE RULE AND THE NATURE OF THE INTERNATIONAL RESPONSIBILITY OF STATES, 35 Ger. Y.B. Int'l L. 9, 12–13 (1992). As Pisillo-Mazzeschi explains, to require some attitude of will, fault or negligence is doomed to fail. Certain situations of international practice would not necessarily be covered by the rules of responsibility. It would be enough to envisage situations where the breach of international obligations is due to situations of error.

100. James Crawford, State Responsibility: The General Part 60–61 (2014). Article 2 of the Draft articles on Responsibility of States for Internationally Wrongful Acts provides "there is an internationally wrongful act of a State when conduct consisting of an action or omission: (a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State"; SEE ALSO Tal Becker, Terrorism and the State: Rethinking the Rules of State Responsibility 136, 139 (2006); Pisillo-Mazzeschi, SUPRA note 98, at 9.

Charter is to prohibit any illegitimate use of force as established by Article 2(4) UN Charter.[101] In *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)*, the International Court of Justice (ICJ) accepted that the Charter provisions concerning the use of force represented customary international law—and even jus cogens.[102] But if there is such a prohibition, the same cannot be said regarding the right of the States to produce, transfer, and develop new armament.[103] Indeed, the doctrines developed in *The Case of the S.S. "Lotus" (France v. Turkey)* and in *Nicaragua* are both applicable on this matter. In the former, the Permanent Court for International Justice (PCIJ) established that "*restrictions upon the independence of States cannot . . . be presumed . . .*" and that international law leaves to States "a wide measure of discretion which is only limited in certain cases by prohibitive rules . . . . [E]very State remains free to adopt the principles it regards as best and most suitable."[104] More importantly and in the same line of argument, the ICJ in *Nicaragua* stated that "in international law there are no rules, other than such rules as may be accepted by the State concerned, by treaty or otherwise, whereby the level of armaments of sovereign state can be limited, and this principle is valid for all states without exception."[105]

The sovereignty of States does include, however, mechanisms to determine the legality of weapons. Indeed, attempts to

---

101. U.N. Charter, art. 2, ¶4. (Article 2(4) UN Charter provides that "all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.").

102. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgement, 1986 I.C.J. 14 ¶ 189–90. (June 27); SEE ALSO Corten, SUPRA note 3, at 209–10.

103. Annyssa Bellal, ARMS TRANSFERS AND INTERNATIONAL HUMAN RIGHTS LAW, IN Weapons and Int'l Hum. Rights L. 448, 448 (Stuart Casey-Maslen ed., 2014).

104. S.S. "Lotus" (Fr. v. Turk.), Judgment, 1927 I.C.J. 10, at 18-19 (Sept. 1927); SEE ALSO George Wendell Berge, THE CASE OF THE S. S. "LOTUS", 26 Mich. L. Rev. 361, 369 (1928).

105. Nicar. v. U.S., 1986 I.C.J., SUPRA note 101, at ¶ 269.

regulate or restrict the use of weapons go back to AD 200.[106] But it was not until the 1949 Geneva Conventions and their 1977 Additional Protocols that processes to determine the legality of weapons received more attention and particularity. Thus, in terms of IHL, as the ICJ argued in the *Advisory Opinion on the Legality of the Threat and Use of Nuclear Weapons*, "all States are bound by those rules in Additional Protocol 1(API) which, when adopted, were merely the expression of the pre-existing customary law, such as the Martens Clause, reaffirmed in the first article of Additional Protocol 1 . . . ,"[107] and that "the intrinsically humanitarian character of the legal principles in question which permeate the entire law of armed conflict . . . applies to *all forms of warfare and to all kinds of weapons, those of the past and those of the future*."[108]

Looking now to the complexity of autonomous technology of warfare, almost every scholar has called attention to the inherent risks of deep learning and the deployment of AWS; each has attended especially to the fact that such systems are *unpredictable systems*[109]—understandably so. In spite of the fact that the *algorithm for the mission* is designed and programmed by human operators, the system actually collects new data and adapts to the uncertainties of the battlefield in real time (*algorithm for situation assessment* and *algorithm for situation management*) in order to optimize one of the possible outcomes (*algorithm for*

106. William H. Boothby, Weapons and the Law of Armed Conflict 9 (2nd ed, 2016).

107. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 84 (July 8) (emphasis added).

108. *Id*. at ¶ 86 (emphasis added).

109. Noel Sharkey, SAYING "NO!" TO LETHAL AUTONOMOUS TARGETING, 9 J. Mil. Ethics 369, 376–81 (2010); SEE ALSO Sharkey, SUPRA note 50, at 24, 32; Noel Sharkey, THE EVITABILITY OF AUTONOMOUS ROBOT WARFARE, 94 Int'l Rev. Red Cross 786, 787 (2012); Krupiy, SUPRA note 29, at 188; Gary E. Marchant, Braden Allenby, Ronald Arkin, Edward T. Barrett, Jason Borenstein, Lyn M. Gaudet, Orde Kittrie, Patrick Lin, George R. Lucas, Richard O'Meara & Jared Silberman, INTERNATIONAL GOVERNANCE OF AUTONOMOUS MILITARY ROBOTS, 12 Colum. Sci. Tech. L. Rev. 272, 283–84 (2011); Dieter Birnbacher, ARE AUTONOMOUS WEAPONS SYSTEMS A THREAT TO HUMAN DIGNITY?, IN Autonomous Weapons Systems: Law, Ethics, Policy 105, 116–17 (Nehal Bhuta, Susanne Beck, Robin Geiß, Hin-Yan Liu & Claus Kreß eds., 2016); Markoff, SUPRA note 86.

target selection). It is important to reiterate that the selection of the optimal outcome is not based on human judgement, but on probabilities.[110] Accordingly, a small mistake by the *algorithm for the situation assessment* or bias can have catastrophic consequences. The situation described above concerning with the Boeing 737 Max accidents are a perfect example.[111] However, in situations where errors cause violations of IHL one must ask how, legally, those violations can be attributed to the State.

First and foremost, the right of States to choose the means and methods of warfare is not unlimited.[112] International law includes both general rules and treaties that prohibit or restrict specific effects, types of weapons, or means and methods of warfare in armed conflicts.[113] As a general rule, customary international law prohibits the use of weapons, means, and methods of warfare that cause superfluous injury or unnecessary suffering, or damage military objectives and civilians or civilian objects without distinction.[114] As a complement, Article 35 and Article

---

110. ICRC, SUPRA note 7, at 10–11; SEE ALSO Krupiy, SUPRA note 29, at 185. (Krupiy considers that another "additional legal criterion" should be added to AWS. There should be an evaluation of the percentage of cases in which the software operated accurately in terms of the laws of targeting. It is possible to question if this criterion would add something new. Indeed, what the author is recognising is the method of probabilities proper of neural networks and the risks inherent to the deployment of AWS.).

111. Bostrom, SUPRA note 52 at 171; SEE ALSO Chesterman, SUPRA note 22 at 240. (SEE SUPRA Section 1.2.).

112. Marco Longobardo, THE RELEVANCE OF THE CONCEPT OF DUE DILIGENCE FOR INTERNATIONAL HUMANITARIAN LAW, 37 Wis. Int'l L. J. 44, 54 (2019).

113. SEE Knut Dörmann & Jose Serralvo, COMMON ARTICLE 1 TO THE GENEVA CONVENTIONS AND THE OBLIGATION TO PREVENT INTERNATIONAL HUMANITARIAN LAW VIOLATIONS, 96 Int'l Rev. Red Cross 707, 708 (2014).

114. ICJ in the NUCLEAR WEAPONS ADVISORY OPINION summarised customary international humanitarian law in 'two cardinal principles.' The first principle enshrines 'THE PROTECTION OF THE CIVILIAN POPULATION AND CIVILIAN OBJECTS AND ESTABLISHES THE DISTINCTION BETWEEN COMBATANTS AND NON-COMBATANTS; STATES MUST NEVER MAKE CIVILIANS THE OBJECT OF AN ATTACK AND MUST CONSEQUENTLY NEVER USE WEAPONS THAT ARE INCAPABLE OF DISTINGUISHING BETWEEN CIVILIAN AND MILITARY TARGETS', and according to the second 'IT IS PROHIBITED TO CAUSE UNNECESSARY SUFFERING TO COMBATANTS: IT IS

36 of the 1977 Additional Protocol to the 1949 Geneva Conventions (Additional Protocol I [API]) provide checks and balances against the possibility of any weapon derogating IHL norms.

As Krupiy rightly points out, numerous parties will be involved in the process of deploying AWS: the deploying State, manufacturers, technicians, military commanders and other human operators.[115] As a consequence, the "collaborative nature of the decision-making related to the architecture of a LAWS poses difficulty for attributing a flawed design of a LAWS to a particular individual."[116] To hold that all IHL violations caused by AWS shall always be attributed to human flaws, as it been argued throughout this Article is not to take the complexity of MLA seriously. Krupiy argues that "in the absence of a sufficiently close link between a human act and an outcome, it would be difficult to argue that any individual would have the necessary mental element for the commission of war crime."[117] However, this Article advances that, in case of errors, it is not simply difficult *but* impossible to establish any possible link of causation between human operators and IHL violations. As Chengeta states "this idea has the chilling effect of throwing the important element of *mens rea* out of the window and putting in place some form of 'strict criminal liability.'"[118] Indeed, any other legal option might well lead to a process which would scapegoat human operators.[119]

ACCORDINGLY PROHIBITED TO USE WEAPONS CAUSING THEM SUCH HARM OR USELESSLY AGGRAVATING THEIR SUFFERING. IN APPLICATION OF THAT SECOND PRINCIPLE, STATES DO NOT HAVE UNLIMITED FREEDOM OF CHOICE OF MEANS IN THE WEAPONS THEY USE.' International Court of Justice (ICJ), SUPRA note 111 at ¶ 78.

115. Krupiy, SUPRA note 40, at 52, 79.

116. *Id*. at 67. (LAWS stands for lethal autonomous weapon systems)

117. *Id*. at 63 (emphasis added). The author, however, seems to have a different understanding elsewhere. SEE Krupiy, SUPRA note 29, at 185–86.

118. Thompson Chengeta, ACCOUNTABILITY GAP: AUTONOMOUS WEAPON SYSTEMS AND MODES OF RESPONSIBILITY IN INTERNATIONAL LAW, 45 Denver J. Int. L. & Pol'y 1, 34 (2016).

119. 2019 GGE Meeting the Government of Brazil, for example, raised concerns about the proposal that commanders should always "be ultimately accountable for violations of IHL during military operations under [their] purview (… [but] factual responsibility must remain

According to Krupiy, liability for AWS should flow from two starting points. First, AWS should be qualified as a "relational entity," and, second, there is always a "dual relation nature" underpinning an AWS deployment which oscillates between the State—the individual government commitment to IHL and decision-making—and a given set of individuals— the programmers, designers, military commanders, etc.[120] It is important to note here that the term "relational entity" is itself questionable from an ontological and conceptual point of view. If AWS were able to establish some kind of relationship, the question as to *why* AWS would not be considered to be moral and intentional agents remains to be answered.[121] The second element, however, is crucial. It is the role of the State to *delegate* operational selection-making in relation to AWS military operations, and at that level of sovereignty, it is the actor responsible for what happens on

---

commensurate with legal accountability, otherwise the human commander operator ends up a mere legal scapegoat in case anything goes wrong." SEE Paula Marshall, Address at the Convention on Certain Conventional Weapons Group of Governmental Experts on Emerging Technologies in the Area of LAWS (Mar. 26, 2019), https://www.unog.ch/80256EDD006B8954/(httpAssets)/122DF2DAEE334DDBC12583CC003EFD6F/$file/Brazil+GGE+LAWS+2019+-+Item+5+a+-+IHL.pdf.

120. Krupiy, SUPRA note 40, at 79–82.

121. The ontological status of AWS goes far beyond the scope of the is work. It is worth mentioning that this issue has been the source of numerous unfortunate discussions. According to the 2011 UK APPROACH TO UNMANNED AIRCRAFT VEHICLES "an autonomous system must not only 'be capable of achieving the same level of situational understanding as a human" but also be "self-aware," and Hin-Yan Liu summed up the question by arguing that the first legal question to be answered is "to whether both autonomous and remote weapons can remain meaningfully categorized as 'weapons', whether the current legal categorization is adequate to regulate their use, and how their use may challenge the existing legal system." SEE UK Ministry of Defence, SUPRA note 49; Hin-Yan Liu, CATEGORIZATION AND LEGALITY OF AUTONOMOUS AND REMOTE WEAPONS SYSTEMS, 94 Int. Rev. Red Cross 627, 628 (2012). However, to understand what AWS as moral agent would imply, SEE Giovanni Sartor & Andrea Omicini, THE AUTONOMY OF TECHNOLOGICAL SYSTEMS AND RESPONSIBILITIES FOR THEIR USE, IN Autonomous Weapons Systems: Law, Ethics, Policy 39–73, 51–58 (Nehal Bhuta, Susanne Beck, Robin Geiß, Hin-Yan Liu & Claus Kreß eds., 2016).

the battlefield.[122] Indeed, when the ICJ held in the *Nuclear Weapons Advisory Opinion* that States' obligation to comply with "the intrinsically humanitarian character of the legal principles in question which permeate the entire law of armed conflict . . . *applies to all forms of warfare and to all kinds of weapons, those of the past and those of the future*."[123] From the decision of the Court, it is possible to conclude, first, that although not all States are parties to the 1977 Additional Protocols, there are customary rules that any State must comply with. Second, the type of weapon is irrelevant in view of the fact that States are obliged to respect their obligations under IHL. Third, and crucially for AWS, the Court seems to establish a direct link of responsibility between the weapon and the deploying State. From the reading of the Court's decision, the attribution is not dependent on the use of the weapon made by its organs or groups acting under the control of the State. The importance of distinct forms of individual responsibility cannot obfuscate that States are the primary recipients of IHL obligations. Therefore, situations in which IHL violations occur cannot be attributed to a human operator, but rather to errors of the system, should fall under the responsibility of the State deploying AWS.[124]

A. States' Due Diligence Obligations. Common Article 1 to the 1949 Geneva Conventions

Some authors, States and organisations argue that the future deployment of AWS should be joined by a treaty regulating those systems.[125] The opportunity for such an agreement is beyond the

---

122. The term "delegation" has two advantages. First, is a term of art among roboticists not to be confused with the legal "delegation", and also it is the term chosen by States at the CCW to refer to the reality of AWS. SEE Sartor & Omicini, SUPRA note 120, at 44–48. SEE ALSO EU STATEMENT GROUP OF GOVERNMENTAL EXPERTS LETHAL AUTONOMOUS WEAPONS SYSTEMS CONVENTION ON CERTAIN CONVENTIONAL WEAPONS (Aug. 28, 2018), https://eeas.europa.eu/delegations/un-geneva/49784/Convention%20on%20Certain%20Conventional%20Weapons%20-%20Group%20of%20Governmental%20Experts%20-%20Lethal%20Autonomous%20Weapons%20Systems_sk..

123. International Court of Justice (ICJ), SUPRA note 111 at ¶ 84; 86.

124. Dustin A. Lewis, Gabriella Blum & Naz K. Modirzadeh, War-Algorithm Accountability 83–84 (2016).

125. Delegations to the CCW have suggested different approaches, among them a legally-binding instrument, a political declaration, or

scope of this article. However, in its current state, IHL already provides a set of obligations for States deploying AWS. This Part will focus on two obligations of due diligence: Common Article 1 to the 1949 Geneva Conventions and Article 36 API.

Due diligence obligations have received particular attention in the context of cyber technology[126] and even the COVID-19 crisis,[127] and such obligations can also play an important role in the implementation of IHL and State responsibility during an armed conflict.[128] However, due diligence, which is sometimes called "one of the most ambiguous terms in terms of international liability and State responsibility[,]"[129] should be clarified.

In general terms, due diligence obligations are primarily connected with States' jurisdiction over its territory and individuals, and are concerned with supplying a standard of care against which fault can be assessed.[130] As articulated in *Corfu Channel (United Kingdom v Albania)* "it is every State's obligation not to allow its territory to be used for acts contrary to the rights of

---

more "clarity on the implementation of existing obligations under international law, in particular IHL." SEE Rep. of the 2018 session of the Group of Gov. Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems 18, U.N. Doc. CCW/GGE.1/2018/3 (Oct. 23, 2018), https://www.unog.ch/80256EDD006B8954/(httpAssets)/20092911F6495FA7C125830E003F9A5B/$file/CCW_GGE.1_2018_3_final.pdf.

126. Hans-Georg Dederer & Tassilo Singer, ADVERSE CYBER OPERATIONS: CAUSALITY, ATTRIBUTION, EVIDENCE, AND DUE DILIGENCE, 95 Int'l. L. Stud. 430–66 (2019); Luke Chircop, A DUE DILIGENCE STANDARD OF ATTRIBUTION IN CYBERSPACE, 67 Int'L. Comp. L. Q. 643, 649 (2018).

127. Antonio Coco & Talita de Souza Dias, PART I: DUE DILIGENCE AND COVID-19: STATES' DUTIES TO PREVENT AND HALT THE CORONAVIRUS OUTBREAK, Blog Eur. J. Int'l L. (Mar. 24, 2020) https://www.ejiltalk.org/part-i-due-diligence-and-covid-19-states-duties-to-prevent-and-halt-the-coronavirus-outbreak/.

128. Longobardo, SUPRA note 111 at, 46–47.

129. SEE Joanna Kulesza, Due Diligence in International Law 1 (2016); SEE ALSO James Crawford, The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries 124 (2003).

130. Duncan French & Tim Stephens, ILA Study Group on Due Diligence in International Law (Second Report) 2 (2016), https://www.ila-hq.org/index.php/study-groups?study-groupsID=63.

other States."[131] According to the International Law Association (ILA), the tri-partite core of due diligence means that (a) a sovereign State; (b) must ensure that within its jurisdiction; (c) other States' rights and interests are not violated'.[132] Hence, due diligence is used to assess the efforts made by a State to prevent certain risks, threats, or harms, including material damage resulting from lawful activities of a State.[133] As Marco Longobardo explains, "obligations of due diligence are not autonomous rules of international law, nor it is a general principle of law, but rather a notion that must be applied in order for the State to comply with some obligations of conduct that embodied in treaty and customary law."[134] In particular, the fact that due diligence is flexible by nature is the reason that it must be a fundament of state responsibility for omissions—at least until State practice or other doctrine establish a better solution.[135]

Particularly relevant for the deployment of AWS is the understanding that a State's due diligence assessment must take into consideration the degree of control exercised by the State over its territory, the State's capacity to produce legislation, and its ability to effectively influence the actions of roboticists, manufacturers, and its own armed forces in order to ensure, as far as possible, that the use AWS will not cause IHL violations.

In light of the above, Common Article 1 of the 1949 Geneva Conventions, commonly framed as an obligation of due diligence, asks States to respect the obligations inherent in the laws of war "in all circumstances." Common Article 1, restated in Article 1API, stipulates that "[t]he High Contracting Parties undertake to respect and to ensure respect for the present Convention in all circumstances."[136]

---

131. SEE Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4 at 22 (Apr. 9). SEE ALSO Kulesza, SUPRA note 129, at 63–64; Chircop, SUPRA note 126 at 649–50; Longobardo, SUPRA note 111, at 51.

132. French & Stephens, SUPRA note 130, at 5–6.

133. Coco & de Souza Dias, SUPRA note 127; SEE ALSO Crawford, SUPRA note 99, at 65.

134. Longobardo, SUPRA note 111, at 53.

135. Kulesza, SUPRA note 129, at 154.

136. SEE Timo Koivurova, DUE DILIGENCE, IN Max Planck Encyclopedias of International Law ¶ 32 (2010) https://ezproxy-prd.bodleian.ox.ac.uk:3405/view/10.1093/law:epil/9780199231690/law-

It has been suggested that common Article 1 has not only a "quasi-constitutional" meaning in current international law, but that it also reflects customary international law.[137] According to the ICRC Study "[a] State's obligation pursuant to this rule is not limited to ensuring respect for international humanitarian law by its own armed forces but *extends to ensuring respect by other persons or groups acting in fact on its instructions, or under its direction or control."*[138] From the reading of Common Article 1, one could conclude that a set positive obligations has indeed been articulated. To start with, the duty "to respect" is in itself a repetition of the rule *pacta sunt servanda*, according to which States commit themselves to comply with IHL framework.[139] Regarding the second duty, as some authors suggest, the term "ensure" phrased in the active voice, indicates that the scope of the obligation to "ensure respect" is broader than simply "not encouraging," and includes a series of positive obligations.[140]

In the *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia*

9780199231690-e1034?rskey=zHswXm&result=1&prd=MPIL; SEE ALSO Dormann & Serralvo, SUPRA note 112, at 708.

137. Jean-Marie Henckaerts & Louise Doswald-Beck, Customary International Humanitarian Law Volume I: Rules 489 (2009). In the NICARAGUA CASE the ICJ stated "there is an obligation on the United States Government, in the terms of Article 1 of the Geneva Conventions, to 'respect' the Conventions and even 'to ensure respect' for them 'in all circumstances,' since such an obligation does not derive only from the Conventions themselves, but from the general principles of humanitarian law to which the Conventions merely give specific expression." SEE Nicar. v. U.S., 1986 I.C.J., SUPRA note 101, at ¶ 220. Carlo Focarelli, COMMON ARTICLE 1 OF THE 1949 GENEVA CONVENTIONS: A SOAP BUBBLE?, 21 Eur. J. Int'L. L. 125, 127 (2010). Henckaerts and Doswald-Beck, SUPRA note 137, at 510–13. Marco Longobardo, THE CONTRIBUTION OF INTERNATIONAL HUMANITARIAN LAW TO THE DEVELOPMENT OF THE LAW OF INTERNATIONAL RESPONSIBILITY REGARDING OBLIGATIONS Erga Omnes AND Erga Omnes Partes, 23 J. Conflict & Sec. L. 383, 390 (2018).

138. Henckaerts & Doswald-Beck, SUPRA note 137, at 496.

139. Longobardo, SUPRA note 111, at 56. (According to Article 26 of the 1969 Vienna Convention of the Law of Treaties, "Every treaty in force is binding upon the parties to it and must be performed by them in good faith.").

140. Dormann & Serralvo, SUPRA note 112, at 727.

and Herzegovina v. Serbia and Montenegro), the ICJ found that the legal obligation enshrined in Article 1 of the 1951 Genocide Convention[141] is one of due diligence, and the considerations of the Court can be of assistance in the interpretation of such obligations and Common Article 1. First, the Court clarified that the term "undertake", present in many international conventions, is not "merely hortatory or purposive" but rather a "formal promise, to bind or engage oneself, to give a pledge or promise, to agree, to accept an obligation."[142] Thus, the obligations to "respect" and to "ensure respect" cannot be considered empty norms since States are under an obligation to "employ all means reasonable available to them" to ensure that its organs and individuals oblige by it.[143] Second, obligations of due diligence need to be assessed *in concreto* according to the possibilities and conditions of each case, because there is no uniformity in the conduct expected of States and International Law has not embraced strict or absolute liability.[144] Third, the breach of an obligation of due diligence requires that a prior violation of International Law has been committed; that is, "a State can only be held responsible for breaching the obligation to prevent genocide only if genocide was actually committed." However, as the Court explained, a "State's obligation to prevent, and the corresponding duty to act, arise at the instant that the State learns of, or should

141. Article 1 of the 1951 Genocide Convention states that "the Contracting Parties confirm that genocide, whether committed in time of peace or in time of war, is a crime under international law which they undertake to prevent and to punish." G.A. Res. 260 A (III), Convention on the Prevention and Punishment of the Crime of Genocide, art. 1, (Jan. 12, 1951).

142. Application of the Convention on the Prevention and Punishment of the Crime of Genocide. (Bosn. & Herz. v. Serb. and Montenegro), Judgment, 2007 I.C.J. 43, ¶ 162 (Feb. 26).

143. Dormann & Serralvo, SUPRA note 112, at 724–25; Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide; Bosn. & Herz. v. Serb. and Montenegro, 2007 I.C.J., SUPRA note 142, at ¶ 430.

144. Bosn. & Herz. v. Serb. and Montenegro, 2007 I.C.J., SUPRA note 142, at ¶ 430; SEE ALSO Longobardo, SUPRA note 111, at 51–52; French & Stephens, SUPRA note 130, at 2.

normally have learned of, the existence of a serious risk that genocide will be committed."[145]

In light of the foregoing, it is possible to apply the same criteria, mutatis mutandis, to States deploying AWS. States are obliged to ensure respect for IHL by employing all means available to guarantee that AWS will be able to comply with IHL. Although, situations of non-compliance will only be detected when autonomous systems cause unpredictable, unlawful outcomes, the obligations of States arise from the moment systems' unpredictability introduce the risk that violations could be committed. The risk element is very important because, from a legal point of view, that risk is permissible, as long the obligations of due diligence are endorsed. Given the risk inherent to AWS, however, higher standards of due diligence should be demand from States from states that deploy such systems. As the ILA noted, the obligations of due diligence should be adaptable to activities that involve increased risks.[146] Accordingly, States should be under specific obligations to use "best efforts to gain knowledge of activity within its territory or jurisdiction", and control every potential risk.[147] An autonomous selection-making process will necessarily demand respect for the "cardinal principles" of IHL[148] and for rules of proportionality, and therefore the

145. Bosn. & Herz. v. Serb. and Montenegro, 2007 I.C.J., SUPRA note 142, at ¶ 431; SEE ALSO Longobardo, SUPRA note 111, at 53.

146. French & Stephens, SUPRA note 130, at 12.

147. *Id*. at 12; SEE ALSO Longobardo, SUPRA note 111, at 51, 63.

148. The ICJ as identified the Principle of Distinction and prohibition to cause unnecessary suffering to combatants as "cardinal principles contained in the texts constituting the fabric of humanitarian law." According to the ICJ those principles are "part of jus cogens as defined in Article 53 of the Vienna Convention on the Law of Treaties of 23 May 1969." SEE Legality of the Threat and Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 78, 83 (July 8). For the complexity of Principle of Distinction and the deployment of AWS, SEE Michael W. Meier, LETHAL AUTONOMOUS WEAPONS SYSTEMS: IS IT THE END OF THE WORLD AS WE KNOW IT . . . OR WILL WE BE JUST FINE?, IN Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare 289, 298–99 (Winston S Williams & Christopher Ford eds., 2019); SEE ALSO Krupiy, SUPRA note 29, at 164–71. Crootof, SUPRA note 23 at 1872–76; Markus Wagner, THE DEHUMANIZATION OF INTERNATIONAL HUMANITARIAN LAW: LEGAL, ETHICAL, AND POLITICAL

deploying States are obliged to prevent by any way possible the occurrence of IHL violations on the battlefield.[149]

B. Common Article 1 and the obligation to "ensure respect." The "Silent Compliance" by States

The interpretation of Common Article 1 is also a source of a continuing debate, particularly regarding the obligation to "ensure respect."[150] The debate is best delineated by asking the following question: According to Common Article 1, are States obliged to ensure respect for IHL only within their jurisdiction, ensuring compliance by their organs and private individuals within their jurisdiction or, much more extensively, are States obliged to actively prevent IHL violations when committed by a third State in a conflict?[151] Under the latter theory, States are obliged to take action against any international actor violating norms of IHL.[152] As the International Criminal Tribunal for the former Yugoslavia (ICTY) explained in *Prosecutor v Krupreskic,*

IMPLICATIONS OF AUTONOMOUS WEAPON SYSTEMS, 47 Vand. J. Transnat'l. L. 1371, 1391 (2014).

149. Arkin, SUPRA note 10, at 186–87. (Article 51(5)(b) and Sub-paragraph (a)(iii) of Article 57 API lays down the rule of Proportionality that prohibits attacks which "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof which is likely to be EXCESSIVE to the concrete and direct military advantage anticipated." Apart of Ronald Arkin who argues from a utilitarian perspective of the rules of proportionality, it is consensual among scholars that proportionality is contextual and demand the exercise of human judgement.). SEE Hum. Rts. Watch, Heed the Call: A Moral and Legal Imperative to Ban Killer Robots 25 (2018), https://www.hrw.org/sites/default/files/report_pdf/arms0818_web.pdf; Ioannis Kalpouzos, DOUBLE ELEVATION: AUTONOMOUS WEAPONS AND THE SEARCH FOR AN IRREDUCIBLE LAW OF WAR, 33 Leiden J. Int'l L. 289, 304–05 (2020); Krupiy, SUPRA note 29 at 160–61, 171–72. SEE ALSO Boothby, SUPRA note 105, at 249; Thompson Chengeta, MEASURING AUTONOMOUS WEAPON SYSTEMS AGAINST INTERNATIONAL HUMANITARIAN LAW RULES, 5 J. L. Cyber Warf. 66, 111–13 (2016); Anderson & Waxman, SUPRA note 43, at 1106; Sassoli, SUPRA note 5 at 10.80 (52122) (With a more optimistic position regarding AI and Proportionality).

150. Longobardo, SUPRA note 137, at 393.

151. Dormann & Serralvo, SUPRA note 112, at 709.

152. *Id*. at 719.

the body of IHL "lays down absolute obligations that are unconditional [and] already encapsulated in Common Article 1 of the 1949 Geneva Conventions, which provides that "[t]he High Contracting Parties undertake to respect . . . the present Convention *in all circumstances*."[153] The court continued that those norms "prohibiting war crimes, crimes against humanity and genocide, are also peremptory norms of international law or *jus cogens*."[154] The understanding of the ICTY, therefore, was that such obligations are owed by all individual States towards the international community, according to which every State ought to "respect" and "ensure respect" of said obligations in all circumstances.[155]

In the last few decades, some authors have suggested that the Common Article 1 is only binding on individual States, and that it does not extend to ensuring that IHL is observed by other States.[156] Be that as it may, it is also true that all scholars agree on the fact that, whatever interpretation of Common Article 1 is taken, that provision demands that States respect, within their jurisdiction, IHL, and, in particular, that its own armed forces, population and those persons and groups whose international wrongdoing can be attributed to the State comply with the attendant obligations.[157] In respect to AWS, this provision has important implications for the deploying State regarding the manufacturers of autonomous warfare technology. The States' duty to observe IHL extends to the manufacture or employment of systems that the State knows or should have known that are incompatible with the duty of the State to respect IHL. Hence, the State must ensure that AWS manufacturers must not entail,

153. Prosecutor v. Kupreki, Case No. IT-95-16-T, Judgment, ¶ 516–17 (Int'l Crim. Trib. for the Former Yugoslavia Jan. 14, 2000).

154. *Id*. at ¶ 520.

155. Focarelli, SUPRA note 137, at 165; Longobardo, SUPRA note 137 at 386; Longobardo, SUPRA note 111, 61–62 n. 82.

156. Taking this position, see Verity Robson, THE COMMON APPROACH TO ARTICLE 1: THE SCOPE OF EACH STATE'S OBLIGATION TO ENSURE RESPECT FOR THE GENEVA CONVENTIONS, 25 J. Conflict & Sec. L. 101, 110 (2020). Longobardo, SUPRA note 137; BUT SEE Dormann & Serralvo, SUPRA note 117, at 709; Focarelli, SUPRA note 137, at 128–29.

157. Robson, SUPRA note 156, at 114; Crawford, SUPRA note 129, at 94–114.

and the deployment of such systems must not result in, a violation of IHL.

According to a 2019 SIPRI report arms, sales of the 100 top largest arms-producing companies amounted to $420 billion in 2018, an increase of 4.6% from 2017. Looking to those with the highest spending on weapons in 2018, all the States interested in the development of AWS, with the exception of China, are listed.[158] The numbers are a sign, not only of the importance of arms sales in terms of international economy, but above all, of the need for States to be obliged to prohibit weapons manufacturers from created systems with the ability to commit IHL violations.[159] It is true that recent European documents, such as the 2017 *OECD's Guidelines on Responsible Business Conduct*[160] and 2019 *Legally Binding Instrument to Regulate, in International Human Rights Law, the Activities of Transnational Corporations and Other Business Enterprises*[161] have reinforced

158. These include Australia, India, Israel, the Russian federation, the UK and the United States. SEE MILITARY EXPENDITURE, Stockholm Int'l Peace Res. Inst., https://www.sipri.org/research/armament-and-disarmament/arms-and-military-expenditure/military-expenditure (last visited May 20, 2020). In what regards China arms sales, it is believed that the weapons industry is State-owned and due to the lack of transparency the real value of the Chinese arm sales is unknown with certainty. SEE ALSO Nan Tian & Fei Su, ESTIMATING THE ARMS SALES OF CHINESE COMPANIES, Sipri insights on peace and security (Jan. 2020), https://www.sipri.org/sites/default/files/2020-01/sipri-insight2002_1.pdf.

159. Kai Ambos, COMPLICITY IN WAR CRIMES THROUGH (LEGAL) ARMS SUPPLIES?, Blog Eur. J. Int'l L. (Jan. 20, 2020), https://www.ejiltalk.org/complicity-in-war-crimes-through-legal-arms-supplies/.

160. OECD, OECD Due Diligence Guidance for Responsible Business Conduct 15 (2018), http://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf.

161. Article 6(1) provides that "State Parties shall ensure that their domestic law provides for a comprehensive and adequate system of legal liability for human rights violations or abuses in the context of business activities, including those of transnational character." SEE Open-ended Intergovernmental Working Group on Transntional Coprorations and Other Business Enterprises with Respect to Human Rughts, REVISED DRAFT LEGALLY BINDING INSTRUMENT TO REGULATE, IN INTERNATIONAL HUMAN RIGHTS LAW, THE ACTIVITES OF TRANSNATIONAL CORPORATIONS AND OTHER BUSINESS ENTERPRISES,

States' commitments towards human rights, but the States' compliance with those commitments is questionable, and States are often silent as far as their obligations are concerned.

The same type of situation can be found in the Arms Trade Treaty (ATT).[162] The ATT reinforces the signatory States' duty of "respecting and ensuring respect for international humanitarian law . . . [and] the responsibility of all States . . . to effectively regulate the international trade in conventional arms."[163] The ATT, to which, for example, all members of the EU, Australia and South Korea are parties, imposes a set of prohibitions on weapons exporters if "the exporting State Party determines that there is an overriding risk . . ." of serious violations of IHL being committed.[164] For these purposes, the ATT requires importing States to provide to the export States all "appropriate and relevant information."[165] Thus, Common Article 1 is vitally important to determine the obligations and responsibility of States to "respect and ensure respect . . ." for IHL. States should ensure, *by all means possible,* that weapons manufactured under their jurisdiction are not exported to places where violations of IHL have been registered.[166]

It is possible to see, however, that present day breaches of those principles abound. For example, it is known that UK suppliers (such as BAE Systems) and American weapons manufacturers (such as Boeing, General Dynamics, Lockheed Martin, Raytheon) have been providing Saudi Arabia with technology

---

art. 6(1) (2019), https://www.ohchr.org/Documents/HRBodies/HRCouncil/WGTransCorp/OEIGWG_RevisedDraft_LBI.pdf.

162. SEE GENERALLY Arms Trade Treaty, G.A. Res. 61/89 (Dec. 24, 2014), https://thearmstradetreaty.org/treaty-text.html.

163. *Id.* at Principles.

164. *Id.* at arts. 6, 7(1)(b)(i), (7)(3).

165. *Id.* at art. 8.

166. Giovanna Maletta, LEGAL CHALLENGES TO EU MEMBER STATES' ARMS EXPORTS TO SAUDI ARABIA: CURRENT STATUS AND POTENTIAL IMPLICATIONS, Stockholm Int'l Peace Res. Inst. (June 28, 2019), https://www.sipri.org/commentary/topical-backgrounder/2019/legal-challenges-eu-member-states-arms-exports-saudi-arabia-current-status-and-potential.

used to target civilians in Yemen[167] in spite of the international acknowledgement of violations of IHL.[168]

---

167. According to the Center for International Policy "Raytheon, Lockheed Martin, Boeing, and General Dynamics were involved in the majority of arms offers notified to [the US] Congress from 2009 through May 2019. In all, the four companies were involved in 27 offers worth over $125 billion, out of a total of 51 offers to Saudi Arabia worth $138 billion. In the recent emergency deal, $4.346 billion of the overall $8.1 billion went to Saudi related arms sales involving one of the top four companies analyzed in this report, including a $1.571 billion deal for the sale and coproduction of Raytheon Paveway bombs and two separate deals totaling $2.6 billion for maintenance and training related to Saudi-owned systems like the Boeing F-15 combat aircraft and the Lockheed Martin C-130 transport plane." SEE Cassandra Stimpson & William Hartung, U.S. Arms Sales to Saudi Arabia: The Corporate Connection 5 (2019), https://static.wix-static.com/ugd/fb6c59_bd62e10ae7b745069e9a6fa897de6a39.pdf. SEE ALSO Michael LaForgia & Walt Bogdanich, WHY BOMBS MADE IN AMERICA HAVE BEEN KILLING CIVILIANS IN YEMEN, N.Y. Times (May 16, 2020), https://www.nytimes.com/2020/05/16/us/arms-deals-raytheon-yemen.html?campaign_id=88&emc=edit_war_20200522&instance_id=18684&nl=at-war&regi_id=93306576&segment_id=28809&te=1&user_id=14348b2c269f57bc16d1502068179d85; Patrick Wilcken, ARMS COMPANIES ARE HIDING BEHIND GOVERNMENTS – IT'S TIME WE HELD THEM ACCOUNTABLE, Amnesty Int'l (Sept. 9, 2019, 12:01 AM), https://www.amnesty.org/en/latest/news/2019/09/arms-companies-must-be-held-accountable/; Dan Sabbagh, BAE SYSTEMS SOLD £15BN WORTH OF ARMS TO SAUDIS DURING YEMEN ASSAULT, The Guardian (Apr. 14, 2020, 1:53 PM), https://www.theguardian.com/business/2020/apr/14/bae-systems-sold-15bn-arms-to-saudis-during-yemen-assault.

168. At the International level, SEE S.C. Res. 2140, ¶ 8 (Feb. 26, 2014); S.C. Res. 2511, ¶ (Feb. 25, 2020); Rep. of the Group of Eminent International and Regional Experts as submitted to the U.N. High Commissioner for Human Rights, SITUATION OF HUMAN RIGHTS IN YEMEN, INCLUDING VIOLATIONS AND ABUSES SINCE SEPTEMBER 2014, ¶ 92, U.N. Doc. A/HRC/42/17 (Aug. 9, 2019) [hereinafter Human Rights Council]. At the European level, SEE Council Decision 2014/932/CFSP, art. 1, 2014 O.J. (L 365); Council Regulation 2015/878, 2015 O.J. (L 143) 1, 2 (EC). In this context, Denmark, Finland, Germany and Netherlands are the only countries which put on halt weapons sales to Saudi Arabia. SEE GERMANY, DENMARK, NETHERLANDS AND FINLAND HALT WEAPONS SALES TO SAUDI ARABIA IN RESPONSE TO YEMEN WAR, NTT News (2018), https://nthnews.net/en/yemennews/germany-denmark-netherlands-and-finland-halt-weapons-sales-to-saudi-arabia-in-response-to-yemen-war/.

The problem of holding weapons manufacturers accountable is not new. Robert H. Jackson's post-war report on the International Conference on Military Trials remarked on the difficulty in identifying the "major war criminals."[169] In the inspiring words of Professor Andre Gros, assistant to the French Judge Roberto Falco, "[s]ome business people should be included in the list of major war criminals . . . ," but in the end, no German weapons manufacturer stood trial at Nuremberg.[170] Today, the situation seems not have improved and the exactly same question of how to hold weapons' suppliers accountable is asked by Professor Kai Ambos.[171]

According to some journalistic investigations, some governments fail to ensure that weapons are not sold to both parties to the conflict.[172] This is not the place to provide a legal analysis on the US use of force in the territory of Yemen,[173] or the liability of

169. Carsten Stahn, A Critical Introduction to International Criminal Law 119–22 (2019).

170. Robert H. Jackson, International Conference on Military Trials 253 (1945), https://www.loc.gov/rr/frd/Military_Law/Jackson-report.html; Mathew Lippman, WAR CRIMES TRIALS OF GERMAN INDUSTRIALISTS: THE "OTHER SCHINDLERS", 9 Temple Int. & Comp. L. J. 173, 176–78 (1995).

171. Ambos, SUPRA note 159.

172. Beth Oppenheim, EUROPE IS AT WAR OVER ARMS EXPORTS, Foreign Pol'y (2019), https://foreignpolicy.com/2019/09/18/europe-is-at-war-over-arms-exports/; Wilcken, SUPRA note 167; Sabbagh, SUPRA note 167.

173. As a short summary, in Yemen, Saudi Arabia and its coalition were invited to use military force by President Hadi in April 2015 to push the Houthis out of Sanaa, Yemen's capital. The US also had the Yemeni government's consent to use force to battle ISIS and al-Qaeda until February 2017. On February 7, 2017 Yemen withdrew its consent for U.S. anti-terror ground missions after children were caught in the crossfire of a firefight between the Navy's Seal Team 6 and suspected terrorists. However, the Yemen government has not withdrew consent for air operations. At present, there is no public information suggesting the government has further restricted consent or reversed its withdrawal of consent for ground operations. Assuming the Yemeni government continues to consent to air operations but not ground operations, then air operations qualify for the consent exception. SEE Amanda Guidero & Maia Carter Hallward, Global Responses to Conflict and Crisis in Syria and Yemen 18–19 (2019). Oona A. Hathaway, Alexandra Francis, Alyssa Yamamoto, Srinath Reddy Kethireddy & Aaron Haviland, THE EXTENT AND VALIDITY OF YEMEN'S CONSENT TO

corporations for violations of human rights.[174] However, it is the present task of this paper to interrogate the responsibility of States which authorize, allow, or ignore weapon sales from private manufacturers which operate in their territories or from State-owned companies. In September 2019, the Panel of Experts for the situation in Yemen recalled that "the obligations of third States to *ensure respect* for international humanitarian law are also particularly relevant . . . for any State that influences or may provide support for parties to the conflict, such as France, the Islamic Republic of Iran, the United Kingdom of Great Britain and Northern Ireland and the United States of America."[175] Though there was no express reference to Common Article 1, the Panel of Experts stated that those States "may well be responsible for providing aid or assistance for the commission of international law violations if the conditions of complicity are fulfilled."[176]

The fact that, in December 2019, the European Center for Constitutional and Human Rights (ECCHR) submitted to the ICC a Communication to investigate the liability of weapons manufacturers as political actors for the war crimes committed in Yemen, is certainly a sign of hope, and might well be a ground-breaking achievement since World War II.[177] The absence of regulation or control over weapons manufacturers operating in a State's jurisdiction should clearly be considered a violations of obligation of due diligence enshrined in Common Article 1. However, as it

---

THE US'S USE OF FORCE, Just Security (Apr. 18, 2018), https://www.justsecurity.org/55066/extent-validity-yemens-consent-us-use-force/.

174. SEE Alex Batesmith, CORPORATE CRIMINAL RESPONSIBILITY FOR WAR CRIMES AND OTHER VIOLATIONS OF INTERNATIONAL HUMANITARIAN LAW: THE IMPACT OF THE BUSINESS AND HUMAN RIGHTS MOVEMENT, IN Contemporary Challenges to the Laws of War: Essays in Honour of Professor Peter Rowe 285 (Caroline Harvey, P.J. Rowe, James Summers & Nigel D. White eds., 2016); Chengeta, SUPRA note 149, at 37–47.

175. Human Rights Council, SUPRA note 168, at ¶ 11, 99(b) (emphasis added).

176. *Id*. at ¶92.

177. SEE MADE IN EUROPE, BOMBED IN YEMEN, European Center for Constitutional and Human Rights (ECCHR), https://www.ecchr.eu/en/case/made-in-europe-bombed-in-yemen/

stands today, independently of the IHL framework, weapons manufacturers seem to be able to operate with or without Governments' approval.

Hopefully, this rather extensive explanation sheds some light on the way in which the deployment of AWS on future battlefield might imply an unsurmountable procedural gap. First, regardless of the values and norms which are sacred under customary and conventional international law, it is simply unclear what Article 1 adds to the other specific provisions found in the 1949 Geneva Conventions or in Additional Protocol I. Second, the lack of attributing State responsibility for violations of weaponry customary and treaty law may well leave Common Article 1 in the plan of a programmatic norm.[178]

C. AWS Legal Reviews. The Enforceability of Article 36 API

The previous section argued that any State has an a priori due diligence obligation to determine whether the study, development, exportation, and importation of AWS would be prohibited by norms of IHL. For this purposes, Article 36 API provides a mechanism for States in order to guarantee that any weapon system, AWS included, will be able to perform lawfully on the battlefield.[179]

Hence, in what concerns new weapons Article 36 API provides that

> 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.[180]

---

178. Focarelli, SUPRA note 142, at 128–129.

179. Kathleen Lawand, Robin Coupland & Peter Herby, Int'l Comm. of the Red Cross, A Guide to the Legal Review of New Weapons, means and Methods of Warfare: Measures to Implement Article 36 of the Additional Protocol I of 1977 3 (2006) [hereinafter International Committee of the Red Cross].

180. Int'l Comm. of the Red Cross, 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 art.

It is debatable if the legal review of new weapons, means, and methods of warfare can be considered a customary obligation of the States, and, moreover, how States are supposed to conduct such reviews. Some authors argue, however, that weapons legal review has customary status.[181] Indeed, the International Committee of the Red Cross Guide to the Legal Review of New Weapons, Means and Methods of Warfare (ICRC Guide) states that "the requirement that the legality of all new weapons, means and methods of warfare be systematically assessed is arguably one that applies to *all* States, regardless of whether or not they are party to Additional Protocol I."[182] As the commentary to the API states "[a]rticle 36 remains, together with the Hague Regulations, the only instrument in the law of armed conflict that can act as a brake on the abuses resulting from the arms race or on the possibility of abuses . . . this article is also concerned with future weapons."[183] However, to highlight the importance of a norm does not state anything about its nature. Indeed, none of the *ICRC Study on Humanitarian Law*, the *Commentary on the API* or the ICJ on *Nuclear Weapons Advisory Opinion* made reference to the possible consuetudinary nature of Article 36 API.[184] To add to this consideration, Article 36 API has been considered non-applicable to other than non-nuclear or conventional

---

36 (1979), https://e-brief.icrc.org/wp-content/uploads/2016/09/11-Article-36-of-Additional-Protocol-I.pdf.Art.

181. Wing Commander Duncan Blake & Lieutenant Colonel Joseph S. Imburgia, "BLOODLESS WEAPONS"? THE NEED TO CONDUCT LEGAL REVIEWS OF CERTAIN CAPABILITIES AND THE IMPLICATIONS OF DEFINING THEM AS "WEAPONS", 66 Air Force L. Rev. 157, 162–63 (2010). Daragh Murray, Practitioner's Guide to Human Rights law in Armed Conflict 172 (Dapo Akanda, Charles Garraway, Françoise Hampson, Noam Lubell & Elizabeth Wilmshurst eds., 2016).

182. A GUIDE TO THE LEGAL REVIEW OF NEW WEAPONS, MEANS AND METHODS OF WARFARE: MEASURES TO IMPLEMENT ARTICLE 36 OF ADDITIONAL PROTOCOL I OF 1977, 88 Int'l Rev. Red Cross, 931, 933 (2006), https://www.icrc.org/en/doc/assets/files/other/irrc_864_icrc_geneva.pdf.

183. Int'l Com. of the Red Cross, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 427 (1987).

184. Henckaerts & Doswald-Beck, SUPRA note 137; International Committee of the Red Cross, SUPRA note 187; International Court of Justice (ICJ), SUPRA note 111.

weapons.[185] What clearly results is that the High Contracting Parties are obliged to determine the legality of the *use* of any new weapons acquired by their armed forces.[186]

Be that as it may, it is important to mention that legal reviews apply to the *intended use of any new weapon* at the time of the evaluation;[187] second, that Article 36 API does not establish the particular way in which the internal procedures for legal reviews must be conducted;[188] third, if a weapon is to be found unlawful the State conducting the review is not obliged to make its findings public;[189] and, fourth, the combined reading of Article 36 API and 84 API is only applicable to States which are party to the 1977 Additional Protocols to the 1949 Geneva Conventions. In this regard, it is interesting to note that very few countries

185. Natalia Jevglevskaja, WEAPONS REVIEW OBLIGATION UNDER CUSTOMARY INTERNATIONAL LAW, 94 Int'l L. Stud. 186, 192 (2018).

186. International Committee of the Red Cross, SUPRA note 179, at ¶ 1479. The Commentary on API establishes that "Article 36 does imply the obligation to establish internal procedures with a view to elucidating the problem of illegality and therefore the other Contracting Parties can ask for information on this point." SEE ID. at ¶ 1482. [THIS IS ALMOST WORD FOR WORD OF WHAT SOURCE SAYS. EITHER PARAPHRASE OR PUT INTO QUOTES. The source reads: According to the ICRC's Commentary on the Additional Protocols, Article 36 "implies the obligation to establish internal procedures for the purpose of elucidating the issue of legality, and the other Contracting Parties can ask to be informed on this point."]

187. Boothby, SUPRA note 105, at 346; International Committee of the Red Cross, SUPRA note 179, at 1479–80; SEE ALSO Vincent Boulanin & Maaike Verbruggen, Stockholm Int'l Peace Res. Inst., Dealing with the Challenges Posed by Emerging Technologies 3 (2017), https://www.sipri.org/sites/default/files/2017-12/article_36_report_1712.pdf.

188. Boothby, SUPRA note 105, at 353; Argentina, FORTALECIMIENTO DE LOS MECANISMOS DE REVISIÓN DE UNA NUEVA ARMA, O NUEVOS MEDIOS O MÉTODOS DE GUERRA 1–5 ¶3 (2018), https://www.unog.ch/80256EDD006B8954/(httpAssets)/9D40986EAE8C70E5C125825F004AD572/$file/CCW_GGE_1_2018_WP.2.pdf; Boulanin & Verbruggen, SUPRA note 187, at 1.

189. International Committee of the Red Cross, SUPRA note 179, at ¶ 1481.

have formal mechanisms for weapons reviews or publish the results of their informal legal reviews.[190]

In light of the above, it is possible to make several conclusions. First, the terms "acquisition" and "adoption" used by Article 36 API are particularly relevant. That provision determines that legal review of new weapons is an early process. The obligation to perform legal reviews applies not only when the nation acquires or adopts a new weapon, but also when the weapon is being studied and developed. Thus, legal reviews must cover all stages of the production of a weapon covering, as far as possible, its anticipated use.[191] According to the USA policy on AWS "*any changes to the system's operating state*—for example, due to machine learning—would require the system to go through testing and evaluation again to ensure that it has retained its safety features and ability to operate as intended [and] in addition to the standard weapons review process, *a secondary senior-level review* is required for LAWS and certain types of semi-autonomous and human-supervised autonomous weapons that deliver lethal effects."[192] Second, the aim of the legal review is to question if the *intended use* of the weapon will disrespect "in some or all the circumstances" rules of International Law. Thus, the weapon "must be tested in circumstances replicating its intended conditions or mode of use . . .," an obligation which arises coherently from Article 1API according to which "the High Contracting Parties undertake to respect and to ensure respect for this Protocol in all circumstances."[193]

---

190. *Id.*

191. Boothby, SUPRA note 110 at 346; A GUIDE TO THE LEGAL REVIEW OF NEW WEAPONS, MEANS AND METHODS OF WARFARE: MEASURES TO IMPLEMENT ARTICLE 36 OF ADDITIONAL PROTOCOL I OF 1977, SUPRA note 182, at 936–37.

192. Cong. Research Service, SUPRA note 14 (emphasis added).

193. Australia, 2018 GROUP OF GOVERNMENTAL EXPERTS OF THE HIGH CONTRACTING PARTIES TO THE CONVENTION ON PROHIBITIONS OR RESTRICTIONS ON THE USE OF CERTAIN CONVENTIONAL WEAPONS WHICH MAY BE DEEMED TO BE EXCESSIVELY INJURIOUS OR TO HAVE INDISCRIMINATE EFFECTS. THE AUSTRALIAN ARTICLE 36 REVIEW PROCESS ¶ 1 (2018), https://unog.ch/80256EDD006B8954/(httpAssets)/46CA9DABE945FDF9C12582FE00380420/$file/2018_GGE+LAWS_August_Working+paper_Australia.pdf. SEE Murray, SUPRA note 181, at 172.

However, the novelty of AWS can in some cases make the process of conducting an Article 36 review very difficult. Legal review of AWS poses new challenges that may themselves require new methods of risk assessment.[194] In other words, how should one conduct a legal review of a system that select its outcomes based in probabilities? Is it possible to design such a review for unpredictable systems of warfare?[195] Gregor Noll expresses these difficulties by questioning

> could we subject any system to a long-term test and see how it performs? In order to have an appropriate testing ground, it is not so much a parallel globe we would require as a parallel history. As we lack one, we cannot be fully sure that we understand how the system works until we use it in a real conflict. Parts of the world, parts of its population, and a particular period in history are put into the wager.[196]

The problem of the appropriate legal review for AWS has been raised by several authors and States.[197] Indeed, as was explained, machine-learning algorithms are only remotely

---

194. Boulanin & Verbruggen, SUPRA note 187, at 6.

195. The ICRC has expressed these concerns early in 2016 stating that "there is a likelihood that increasingly autonomous weapon systems could become less predictable, particularly in case of increased mobility, increased adaptability and/or increased interaction of multiple systems (as swarms). The loss of predictability regarding the outcomes of using an autonomous weapon may point to the loss of human control over that weapon's operation, with human decision-making over the use of force being replaced by machine processes." SEE AUTONOMOUS WEAPONS: DECISIONS TO KILL AND DESTROY ARE A HUMAN RESPONSIBILITY, Int'l Committee Red Cross (Apr. 11, 2016), https://www.unog.ch/80256EDD006B8954/(httpAssets)/9324B81015529E3DC1257F930057AF12/$file/2016_LAWS+MX_GeneralExchange_Statements_ICRC.pdf.

196. Noll, SUPRA note 40, at 88–89.

197. Jakob Kellenberger, ICRC Predisent, Keynote Address at the International Humanitarian Law and New Weapon Technologies, 34th Round Table on Current Issues of International Humanitarian Law (Sept. 8, 2011), IN 94 Int'l Rev. Red Cross 809, 810 (2012); Heather M. Roff & David Danks, "TRUST BUT VERIFY": THE DIFFICULTY OF TRUSTING AUTONOMOUS WEAPONS SYSTEMS, J. Mil. Ethics 1, 3–4 (2018), https://doi.org/10.1080/15027570.2018.1481907; Argentina, SUPRA note 192 at ¶ 5.

predictable, and there are elements that cannot be controlled a prior, simply because they are unknown at the time of testing a system.[198] As Stuart Russell, a professor of computer science, clarifies, "the feasibility of autonomous weapons is also not in question, at least for a broad class of missions that might currently be contemplated . . ., and discrimination is probably feasible in most situations." However, he underlines, "determining proportionality and necessity is probably not feasible for current AI systems and would have to be established in advance with reasonable certainty by a human operator, for all attacks that the weapons might undertake during a mission."[199]

Looking at the statements and working papers submitted to the CCW, several States have sought to address the importance of legal reviews to ensure AWS' legality.[200] For the purpose of

198. As the Holy See stated at the GGE "if one delegates important decision-making powers to a machine whose behavior is unpredictable or whose field of operation is not well-defined or known (i.e., it has machine learning capabilities), the crucial action/responsibility nexus would be inevitably jeopardized." SEE Holy See, STATEMENT BY THE PERMANENT MISSION OF THE HOLY SEE TO THE UNITED NATIONS AND OTHER INTERNATIONAL ORGANIZATIONS IN GENEVA AT THE (2018), https://www.unog.ch/80256EDD006B8954/(httpAssets)/E3015FACDD8757B4C12582F800595E37/$file/2018_GGE+LAWS+2_6a_Holy+See.pdf (last visited Sep 12, 2018).

199. Stuart J. Russell, Prof. of Computer Science, U.C. Berkley, AI AND LETHAL AUTONOMOUS WEAPONS SYSTEMS, Remarks Delivered at the Meeting of the Group of Governmental Experts on Lethal Autonomous Weapons Systems, Geneva (Nov. 13, 2017), https://people.eecs.berkeley.edu/~russell/research/LAWS/russell-ccw17-GGE-remarks-written-2017-11-13.pdf.

200. From 2016 until 2020 CCW Meeting of Experts on Lethal Autonomous Weapons, with the exception of China and India, States' representatives (among them Argentina, Australia, Belgium, Canada, France, Germany, Israel, Japan, Mexico, the Netherlands, Poland, Russia, Sierra Leone, South Africa, Sweden, the UK and the US) endorsed the proposition that the review process be regarded as crucial in ensuring that AWS are lawful and are used lawfully. Some other States, such as Zambia and Finland, that argue that "national reviews are insufficient to deal with LAWS" and support of "creating international standards for the implementation of this norm [Article 36 API]." At the same time some States – Australia, Belgium, Germany, Israel, Sweden, the UK and the US – provided explanations and/or updates of their weapons review processes. SEE Chris Jenks & Lt. Col. Chris Ford, THE INTERNATIONAL DISCUSSION CONTINUES: 2016 CCW EXPERTS MEETING ON LETHAL AUTONOMOUS WEAPONS, Just Security (Apr. 20,

this article, two are particularly relevant: two statements presented by Argentina in 2018 and 2019, and one by Australia in 2018.[201] Both States aim to reinforce the importance of legal reviews, such as those required by Article 36 API and, at the same time, that there can be legal reviews suitable for AWS.[202] Nonetheless, Argentina and Australia have different approaches to the matter. Argentina, on one hand, insists on the internationalisation of the obligations enshrined in Article 36 API and Article 84 API. Argentina considers that the obligation to examine the legality of any new weapon became "universal" with the implementation of Article 36 API, recognising at the same time that "the implementation at national level remains still weak and ambiguous."[203] Thus, according to Argentina, two sets of a priori obligations should be established for two different groups

---

2016), https://www.justsecurity.org/30682/2016-ccw-experts-meeting-laws/. SEE GENERALLY https://www.unog.ch/80256EE600585943/(httpPages)/37D51189AC4FB6E1C1257F4D004CAFB2?OpenDocument; Zambia, 'Zambia's Statement at the Informal Meeting of Experts on Lethal Autonomous Weapons System (LAWS)'<https://www.unog.ch/80256EDD006B8954/(httpAssets)/2927422250D59E8EC1257F920057EDB5/$file/Zambia+Statement+at+the+meeting+of+Experts+on+LAWS.pdf>. Finland, FINLAND STATEMENT AT MEETING OF EXPERTS ON LAWS 11-15 APRIL, 2016 (2016), https://www.unog.ch/80256EDD006B8954/(httpAssets)/999D215ACBAD2C8BC1257F920057F580/$file/2016_LAWS+MX_GeneralExchange_Statements_Finland.pdf.

201. Argentina, SUPRA note 192; Argentina, QUESTIONNAIRE ON THE LEGAL REVIEW MECHANISMS OF NEW WEAPONS, MEANS AND METHODS OF WARFARE (2019), https://www.unog.ch/80256EDD006B8954/(httpAssets)/52C72D09DCA60B8BC125841E003579D8/$file/CCW_GGE.1_2019_WP.6.pdf; Australia, SUPRA note 197.

202. Argentina, SUPRA note 192; Argentina, SUPRA note 205; Australia, SUPRA note 197.

203. Argentina (n 27)¶ 2; 5. This position is questionable if the obligation does not have customary character, and more so when Argentina considers that the right of combatants to choose their means and methods of warfare is not unlimited (Article 35 API) is of "character of Jus Cogens." The ICJ Advisory Opinion on Nuclear Weapons qualified rather the prohibition of indiscriminate weapons and principle of distinction as "intransgressible principles of international customary law". International Court of Justice (ICJ), SUPRA note 111 at ¶ 79; 83.

of States, *manufacturers* and *importers*, in order to determine if AWS have any "technical analytical deficiencies."[204] Aside from the national obligation to proceed to legal reviews, a State could delegate all the necessary procedures of a review in more technically capable states.[205] Argentina also insists on the importance of the obligation stipulated by Article 84 API, according to which States should share the technical procedures they adopt to legitimise AWS, but with no obligation to share the results of such tests.[206] In 2019, Argentina suggested at the *Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems* (GGE) that a questionnaire be distributed among States to enquire into the kind of legal reviews that States have embraced, and to be returned to the Argentinian Government.[207]

Australia, on the other hand, opted for a more modest proposal that requires sharing with the other States party to the CCW how, when, and who is to conduct legal reviews that ensure a new weapon, such as AWS, complies with Australia's international obligations.[208]

In light of the above, it is possible to conclude that "[i]f legal weapons reviews are to be effective, it is necessary to verify that States conduct them appropriately – Information-sharing mechanisms need a boost [and] . . . [r]educing the reach of the confidentiality shield is essential; otherwise, weapons development will not only drive the development of the law, it will continue to curtail the application of the law as it already exists."[209]

However, and in spite of all goodwill manifested by several States and claims made by scholars, one fact remains unsurmountable. States' sovereignty is of paramount importance,

---

204. Argentina, SUPRA note 192 at¶ 7-8.

205. *Id.* at ¶ 5.

206. *Id*. at 9.

207. Argentina, SUPRA note 205 at ¶ 5-6.

208. Australia, SUPRA note 197 at ¶ 4, 8, 9, 11.

209. Marcos Kotlik, REVIEWING LEGAL WEAPONS REVIEWS: IS IT POSSIBLE TO VERIFY COMPLIANCE?, Blog Eur. J. Int'l L. (Mar. 19, 2020), https://www.ejiltalk.org/reviewing-legal-weapons-reviews-is-it-possible-to-verify-compliance/?utm_source=mailpoet&utm_medium=email&utm_campaign=ejil-talk-newsletter-post-title_2.

which is confirmed by international jurisprudence.[210] AWS' legal reviews are national domestic process in which secrecy is protected by law since "the High Contracting Parties are not bound to reveal *anything* regarding new weapons which are being developed or manufactured."[211]

As explained above, it would be legally impossible to impose an obligation on States that are not contemplated in the norms of international law. Nonetheless, it may be argued that, looking to the behaviour and practice of States at the CCW regarding compulsory legal reviews, Article 36 API is acquiring some level of *opinio juris*, at least regarding AWS. The essence of custom according to Article 38 of the statute of the ICJ is that it should constitute evidence of a general practice accepted as law. As the ICJ noted in the *Advisory Opinion on Nuclear Weapons* the "substance of customary law must be looked for primarily in the actual practice and *opinio juris* of states."[212] The problem "is how to distinguish behaviour undertaken because of a law from behaviour undertaken because of a whole series of other reasons[, such as] from ideological support to political bribery."[213] The element of practice would be easier to address if the most important manufacturers and importer States undertake legal reviews as a new , reiterative practice. The second element, that "evidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it . . ." appears to be frustrated by practical impossibility.[214] It will depend on how other States react as to whether a new customary norm emerges or not. In the specific case of the negotiations at the CCW concerning AWS, it is possible to see some factors that could cause

---

210. International Court of Justice (ICJ), SUPRA note 111 at ¶ 27. Another example can be offered. The Arms Trade Treaty (2014), in its Preamble reaffirms "the sovereign right of any State to regulate and control conventional arms exclusively in its territory, pursuant to its legal and constitutional system." SEE The Arms Trade Treaty, SUPRA note 162, at Preamble, ¶ 4.

211. International Committee of the Red Cross, SUPRA note 179, at ¶ 1481 (emphasis added).

212. International Court of Justice (ICJ), SUPRA note 111, at ¶ 64.

213. Malcolm N. Shaw, International Law 75 (6th ed. 2008).

214. North Sea Continental Shelf (Ger./Den.; Ger./Neth.), Judgment, 1986 I.C.J. 3 ¶ 77 (Feb. 20)].

difficulties for a new legal practice. The Russian Federation, for example, assures that it "has put in place a state-wide system to check prototypes for compliance . . . carried out at all stages of development of prototype weapons and military equipment, as well as during their operation' but it 'deems it *unnecessary to elaborate a universal mandatory mechanism for "legal reviews"*, especially just for LAWS."[215]

Faced with the difficulties mentioned above, it seems that the obligation provided on Article 36 API is not safe ground to guarantee AWS' compliance with IHL for two reasons. First, it seems difficult, if not impossible, to envisage Article 36 API as a norm of customary international law for conventional weapons enforceable against States; second, looking at the statements presented at the CCW meetings, States are themselves reluctant to adopt regimes of more "strict tolerance" to future AWS.

CONCLUSION

IHL has long been developing consuetudinary and conventional norms in order to establish limits on the way States deploy new means and methods of warfare, and more specifically, how weapons can be used on the battlefield. Roboticists have the task of proving that those limits can be encoded in the *algorithm for the mission*. It is not the role of lawyers to question what technology can or cannot achieve. However, roboticists recognize that MLA will introduce a level of unpredictability not known until today on the battlefield. The possibility of AWS making errors on the battlefield raises questions as to who might be held accountable when the system causes unlawful consequences. In these types of situations, the deploying State should bear responsibility for delegating on AWS missions that, in the past, required the presence or supervision of human operators. The State is always responsible for all the weapons that their armed forces deploy on the battlefield, as stated by international jurisprudence.

Dealing with the unpredictability of AWS, and possibility of errors, does not represent itself an unsurmountable obstacle from an IHL point of view. However, in matters involving weapons, States tend to neglect their conventional obligations—creating true procedural gaps. In terms of AWS, this can represent

215. The Russian Federation, SUPRA note 29, at ¶ 8–9 (emphasis added).

a doomed future for IHL. The possibility of States considering errors as malfunctions is an accountability trap, since no one can be blamed for malfunctions and they fall within the category of "permissible malfunction blameworthiness gap." Thus, instead of an accountability gap, this article argues that the real problem regarding the deployment of AWS is the fact that States, in matters of weaponry, tend to *fall silent*. This silence means, in the long run, violations of fundamental principles of IHL will simply be considered as unfortunate accidents on the battlefield. The future looks indeed gloomy if States opt for the deployment of AWS without being compliant with their well-established international obligations. In the specific case of AWS, it is imperative to recognize the category of errors in order to guarantee that States are committed with the values enshrined in the IHL body.