TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Aleksi Kajander

Making the Cyber Mercenary - Autonomous Weapons Systems and Common Article 1 of the Geneva Conventions

Master's thesis
Programme HAJM, specialisation Law and Technology

Supervisor: Agnes Kasper, Senior Lecturer
Co-supervisor: Evhen Tsybulenko, Senior Lecturer

Tallinn 2020

I declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously been presented for grading.
The document length is 17 988 words from the introduction to the end of conclusion.

Aleksi Kajander ……
(signature, date)
Student code: 184733HAJM
Student e-mail address: Aleksi.kajander@gmail.com

Supervisor: Agnes Kasper, Senior Lecturer:
The paper conforms to requirements in force

……
(signature, date)

Co-supervisor: Evhen Tsybulenko, Senior Lecturer:
The paper conforms to requirements in force
……
(signature, date)

Chairman of the Defence Committee:
Permitted to the defence
……
(name, signature, date)

TABLE OF CONTENTS

Abstract:

Common Article 1 of the Geneva Conventions requires that states ‘respect and ensure respect’ for the Geneva Conventions ‘in all circumstances’. In the new 2016 Commentary the existence of not only a negative obligation, but also a positive obligation on third countries to a conflict to prevent violations was confirmed. Hence, third countries must do everything ‘reasonably in their power to prevent and bring such violations to an end’.

Autonomous weapons systems (AWS) are already being used as exemplified by various missile defense systems. Consequently, inevitably a state that is buying or being supplied with AWS will use them in a conflict. Therefore, suppliers of such systems will have to comply with the aforementioned positive obligation.

This thesis will examine the positive obligation’s impact on AWS and the state supplying them. These include the question of will it be their responsibility to ensure the system cannot violate the Geneva Conventions and take measures to prevent violations. Chief among these potential measures being the possibility of the supplying states maintaining a permanent tether enabling the remote influencing of the AWS. The implications of tethering the supplied AWS may go well-beyond ensuring compliance with IHL, including multiplying the leverage of the supplying state by turning the system into ‘cyber mercenaries’.

The structure of the thesis will therefore be essentially two-fold. Firstly, the positive obligation contained in the new commentary will be analyzed and then secondly, applied to the case of AWS sold by third countries to a conflict.

Keywords: *autonomous weapons, geneva convention, international humanitarian law, IHL*

Introduction

The advance of autonomous technology is raising questions and shifting paradigms in a variety of fields such as transport, business and even governance. The military is no exception to this trend as the possibilities for the military uses of autonomous technology are becoming increasingly apparent. However, like other fields, the existing framework of laws was not created with autonomous systems in mind, and therefore its application to such systems is unclear. Nevertheless, in the case of the military application of autonomous weapons systems (AWS), the application of the existing rules is literally a matter of life-and-death.

The Geneva Conventions have long been held a cornerstone of international humanitarian law, and their application and interpretation have had fundamental effects on conflicts since their introduction[1]. The four Geneva Conventions address a wide variety of problems arising from land, air or naval warfare including the protection of civilian populations and objects[2]. With the introduction of AWS, the Geneva Conventions are now having to be examined in a new light, which creates new legal questions about their application.

In this regard, an updated commentary was released on the First Geneva Convention in 2016, which confirmed the existence of a positive external obligation in relation to Common Article 1, whereby the High Contracting Parties 'undertake to respect and ensure respect' for the Convention in 'all circumstances'[3]. This positive obligation requires that the High Contracting Parties do 'everything reasonably in their power to prevent and bring such violations to an end'[4].

This positive external obligation reaches a whole new dimension with the introduction of AWS, as a contracting party supplying them could potentially have unprecedented control over their supplied systems, be it by their programming or by the presence of a 'backdoor' enabling remote

[1] Cameron, L.,Demeyere, B., Henckaerts, JB., La Haye, E., Niebergall-Lackner, H. (2015). The updated Commentary on the First Geneva Convention – a new tool for generating respect for international humanitarian law. *International Review of the Red Cross*, Vol. 97 (900) ICRC 97, 1210.
[2] Alston, P., Steiner, H., Goodman, R. (2008). *International Human Rights in Context*. (3rd ed) Oxford: United Kingdom, Oxford University Press, 70.
[3] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention), 12 August 1949, 75 UNTS 31, Article 1.
[4] International Review of the Red Cross, *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 2nd edition, 154.

control. Hence, in either case significantly improving their ability to prevent IHL violations. However, the latter type of tethering, if required by Common Article 1, could bring besides added compliance a new dimension to cyber warfare as well as have unintended military and political effects. Therefore, ‘backdoors' are a double-edged sword in the sense that while they may bring added compliance, they will bring additional risk factors in the form unintended third parties gaining access to the AWS.

Therefore, the defining the contents of this positive external obligation will be of utmost importance for the states supplying such AWS, as it will impact both the design of those systems as well as the circumstances in which they can be supplied. This thesis aims to analyze the relationship and implications of the positive external obligation in Common Article 1 in relation to AWS and the states supplying them, especially whether the supplying state is obliged to maintain a tether to supplied systems. From which the research question of the thesis is derived, which is how will the positive obligation of third nations to prevent violations of IHL of Common Article 1 of the Geneva Conventions be applied to autonomous artificial intelligence weapons systems?

Consequently, to address the research question and accomplish the aim of the thesis, the structure of the thesis is broadly divided into three distinct parts. The first part examines and analyzes Common Article 1 of the Geneva Conventions, including its various interpretations, which will lay the foundation for the later analysis in the context of autonomous weapons systems. Furthermore, the first section will discuss what the potential measures required by Common Article 1 could be in relation to autonomous weapons systems, which will form a basis for the later discussion in the third section.

The second part of the thesis discusses the nature of autonomous weapons technology and its key aspects that must be taken into account when considering how those systems should be legally regulated. Moreover, the second section is crucial in establishing an understanding as to what is practically feasible and reasonable in the light of the technology in regard to its regulation.

The third section combines the considerations of the first two sections into an analysis of how Common Article 1 interacts with autonomous weapons systems. The section culminates in the analysis of the two possible models for autonomous weapons systems in relation to autonomous

weapons systems, that is to say, whether they are tethered to the state of origin to prevent violations of IHL and thus, ensure respect for those norms.

The critical analysis of legal acts and policy documents is the principal method for the research, as the aim of the thesis is to ultimately apply the positive obligation contained in Common Article 1 of the Geneva Conventions to autonomous weapons systems. Therefore, in order to achieve this, it is absolutely necessary to analyze the legal acts themselves as well as their related documents such as the 2016 Commentary and travaux preparatoires to be able to define the scope and content of the positive obligation, and ultimately apply it to the autonomous weapons systems.

Moreover, the review of relevant case law will additionally be used to establish how similar obligations have been applied and new weapons systems treated in the past, in terms of international law. Of course, the actual direct case law of autonomous weapons systems will be somewhat limited as such devices have not yet been introduced on a large scale. Nonetheless, examination of how Common Article 1 has been applied in the past as well as how new weapons systems have been treated under international law, will arguably be indicative of how decisions makers will approach them in the future.

In addition, the conceptual analysis method is used to meet the objective of applying the positive obligation contained in Common Article 1. For, relevant related concepts such as due diligence and ‘reasonable’ means must be analyzed, as they are crucial to defining the scope of the obligation contained within Common Article 1. Therefore, based on the above, the research will mainly use qualitative methods.

1. Common Article 1

1.1. Introduction to Common Article 1

Common Article 1 (CA 1) derives its name from being the first article of all four 1949 Geneva Conventions, consequently it forms a prominent part of the Geneva Conventions which are considered the cornerstones of International Humanitarian Law (IHL)[5]. The provision itself is an evolution of Article 25 of the 1929 Geneva Convention which is similarly worded that also obliges High Contracting Parties (HCPs) to respect the Convention in 'all circumstances'[6]. For the 1949 version that is now called Common Article 1, the wording was changed and the Article itself given more prominence by placing it as the very first Article, with the intention of strengthening it when compared to the 1929 Article[7].

Like all international law articles, CA 1 is interpreted in accordance with the Vienna Convention on the Law of Treaties (VCLT) Articles 31 and 32. As a result, it is primarily interpreted through the 'ordinary meaning' of the terms in their context and 'in the light of the objective and purpose of the treaty' in accordance with Article 31 of the VCLT. In the case of ambiguities or absurd results, the supplementary means of interpretation are used to determine the meaning of the provision, which includes the Commentaries to the Article. Common Article 1 has two commentaries attached to it, the earlier 1952 and the recent 2016 Commentary. The 2016 Commentary confirmed the existence of the long-debated positive external obligation for HCP to prevent violations and bring existing violations of IHL by other parties to an end, thus arguably bringing the most drastic change in the interpretation of the Article since the 1952 Commentary.

At its core, Common Article 1 has a two-fold structure, the first of which is to restate the principle of *pacta sunt servanda*, the binding nature of the treaty and the obligation of the parties

[5] Cameron, L., Demeyere, B., Henckaerts, JB., La Haye, E., Niebergall-Lackner, H. (2015). The updated Commentary on the First Geneva Convention – a new tool for generating respect for international humanitarian law. *International Review of the Red Cross*, Vol. 97 (900) ICRC 97, 1210.
[6] Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field. Geneva, 27 July 1929.
[7] Commentary of 1952 Convention (I) for the Amelioration of the Condition of the Wounded and Sick in armed Forces in the Field. Geneva, 12 August 1949.

to perform the treaty obligations in good faith[8].This first obligation is evidenced by the wording of the Article whereby all High Contracting Parties 'undertake to respect' the convention in all circumstances. The first obligation is therefore relatively straightforward and unambiguous, to ensure that the party performs their own obligations in good faith and respects the Conventions and the entire body of international humanitarian law binding upon that state. The reference to 'all circumstances' clarifies that the obligations of CA 1 are always applicable during both peace and more exceptional circumstances, which is a view confirmed by the 2016 Commentary[9].

The second obligation derives from the addition of the words 'and to ensure respect' for the Convention, which read in combination with the first obligation could conceivably be directed externally, to include an obligation to ensure the compliance of other states as well. This second obligation represents the biggest change from the 1929 Article 25 as it did not include the second obligation of ensuring respect. However, the second obligation is far more ambiguous, as arguably there are many ways of 'ensuring respect', and moreover, the scope of this obligation may be argued as whether it includes an external dimension regarding the compliance of other states. Hence, the second obligation to 'ensure respect' for the Convention in all circumstances would go beyond the ordinary principle of *pacta sunt servanda* in the sense that the parties not only have the obligation to perform their own obligation in good faith, but additionally to make sure that others do so as well[10].

However, when examining the older 1952 Commentary the meaning of the obligation to 'ensure respect' was not necessarily intended to include such an external obligation. Instead, the 1952 Commentary makes reference to the idea that the wording was used to 'emphasize and strengthen' the responsibility of the HCP whereby it would not be sufficient that they merely instruct their civilian or military authorities, but rather that the state should additionally supervise their execution[11]. As a second aspect, the state should take preparatory measures in advance, i.e. during peacetime, to ensure that when the time comes the Convention will be adhered to[12]. Therefore, as both of these obligations are nonetheless directed solely towards the HCP itself and

---

[8] International Review of the Red Cross, *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 2nd edition, 143.
[9] Ibid., 185.
[10] Ibid., 154.
[11] International Review of the Red Cross, *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 1st edition.
[12] Ibid.

not other parties, it can and has been argued that the obligation is not directed towards other parties besides the HCP[13].

Nevertheless, even the 1952 Commentary includes a statement regarding a situation where a party is failing to adhere to its obligations, in which case the other HCPs, be they neutral, allied or enemy, 'may and should' endeavor to ensure that party returns to complying with its obligations[14]. However, the use of the more voluntary wording 'may and should' as opposed to using the compulsory wording of 'shall' could be argued to indicate that this obligation is not obligatory unlike the aforementioned internal aspects. By contrast, the 2016 Commentary uses the obligatory wording of 'must' in a sentence reminiscent of the 1952 Commentary, requiring 'neutral, allied or enemies' to do everything 'reasonably' in their power to 'ensure respect' to the convention by those 'Party to a conflict'[15]. Consequently, the 2016 Commentary is explicit in stating that the obligation to 'ensure respect' includes a positive obligation to do 'everything reasonably' in the power of that HCP to prevent and end violations by other parties, thereby removing doubt as to its binding nature[16].

As pointed out by the 2016 commentary, the meaning of the term 'ensure' is to make sure something will occur or inversely that something will not occur, i.e. in this case violations of the Conventions[20]. As the scope is not qualified in the text of CA 1 itself, in the sense that it is not mentioned whether the obligation to 'ensure respect' is directed internally solely at the HCP itself or it includes an external dimension towards other parties, it could reasonably be considered that the wording would include both an external and internal dimension. Therefore, logically this obligation would go beyond the prohibition to encourage, aid or assist violations of the Convention by parties to a conflict which is an undisputed part of Common Article 1[21].

---

[13] Zych, T. (2009). The Scope of the Obligation to Respect and to Ensure Respect for International Humanitarian law. *Windsor Yearbook of Access to Justice*, Vol. 27,270.
[14] International Review of the Red Cross, *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 1st edition.
[15]International Review of the Red Cross, *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 2nd edition, 153.
[16] Ibid., 153.
[20] Ibid., 145.
[21] Clapham, A., Gaeta, P., Sassoli, M., (2015). *The 1949 Geneva Conventions: A Commentary*. (1st ed.) Oxford: United Kingdom: Oxford University Press, 130.

Therefore, based on the 2016 Commentary, on the one hand, ensuring respect within the meaning of CA 1 includes a preventive aspect, whereby the HCPs must take steps to prevent foreseeable violations, both during peace and wartime, which as mentioned above is directed additionally towards other parties such as those in a conflict. On the other hand, the positive obligation requires that the HCP does 'everything reasonably in their power to…. bring such violations to an end[22]'.

In relation to preventing future violations, it is necessary that there is a foreseeable risk of them being committed[23]. The actual means by which a state is to carry out this obligation is largely at their discretion, provided the principle of due diligence is adhered to[24]. Hence, the positive external duty to ensure respect is an 'obligation of means', whereby a HCP is not held responsible for a failure of their efforts, provided they did everything reasonably in their power[25]. Consequently, the HCP must first correctly identify foreseeable violations in the future, and then take all the measures reasonably in their power to prevent them.

The 2016 Commentary goes on to refer particularly to the 'unique position' to influence where a HCP takes part in the arming, training or otherwise equipping the armed forces of a Party to a conflict[26]. If we consider autonomous weapons systems in this context, it is apparent that if a HCP is providing such weapons they are arguably in an even more unique of a position to prevent and bring violations to an end, as they could reasonably have taken a multitude of steps to increase their influence beforehand, such as placing remote 'kill-switches' on the supplied systems. Arguably, this is thus the first time the use of physical weapons systems in the physical possession of another state that they were supplied to, can be made conditional on complying with IHL, even if conceivably similar conditions could already in the present be attached to the use of cyber capabilities supplied by another state.

Therefore, whereas in the case of conventional human operated weapons the most the supplying party could do directly in relation to them, is to threaten to or to stop further supply. Under the

---

[22] International Review of the Red Cross, *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 2nd edition,154.
[23] Ibid., 164.
[24] Ibid., 165.
[25] Ibid., 165.
[26] Ibid., 167.

new paradigm, the threat could be to make existing systems useless, thus greatly increasing the leverage. Moreover, this would effectively prevent future violations, at least by those AWS that can be disabled. Which both introduces the importance and leads us to the main topic of this paper, what are the implications of Common Article 1 in relation to a High Contracting Party supplying autonomous weapons systems and are they required to maintain a tether enabling control of those supplied systems?

1.2. The Means of Interpreting Common Article 1

The value of any legal provision is in its interpretation, which is true for Common Article 1 as well. As it is an international treaty provision, it is to be interpreted in accordance with the Vienna Convention on the Law of Treaties (VCLT) Article(s) 31-33. Consequently, the correctness of an interpretation is determined in reference to the VCLT[27]. However, there is dispute even about exactly how the interpretation process is to be carried out, with advocates for considering interpretation an art or craft, whereas those opposed argue the interpretation is to be carried out in reference to an extensive and exhaustive list of implicit or explicit guidelines[28].

Nonetheless, under the VCLT the primary means of interpretation are contained within Article 31 with the first paragraph acting as the center of gravity, whereby a provision 'shall' be interpreted in 'good faith' and 'in accordance with the ordinary meaning' of the terms 'in their context and in the light of its [treaty] objective and purpose'[29]. Often in practice, for the purposes of interpretation there may not be cause to look further, however, if additional elements such as subsequent practice are present, then it may be necessary to proceed further down the Article such as to 31 (3) (b) concerning subsequent practice[30]. Consequently, Article 31 does not warrant a purely literal interpretation owing to the inclusion of considerations of the 'object and purpose' of the treaty, however, nonetheless the primary means of interpretation remains textual.

---

[27] Linderfalk, U. (2007). Is the Hierarchical Structure of Article 31 and 32 of the Vienna Convention Real or Not? Interpreting the Rules of Interpretation. *Netherlands International Law Review*, Vol. 54(1), 134.
[28]Mcgrogan, D. (2014), On the Interpretation of Human Rights Treaties and Subsequent Practice. *Netherlands Quarterly of Human Rights*, Vol. 32(4), 350-351.
[29] Herve, A. (2016). Article 31 of the Vienna Convention on the Law of Treaties and Investment Law. *ICSID Review- Foreign Investment Law Journal*, Vol. 31(2), 370.
[30] Ibid.

Should Article 31 produce an ‘ambiguous or obscure’ or ‘manifestly absurd or unreasonable’ result, recourse ‘may’ be had to Article 32 which provides the ‘Supplementary’ means of interpretation. Under the wording of Article 32 the named supplementary means of interpretation include the ‘preparatory work’ of the treaty as well as the ‘circumstances of its conclusion’, which may be used to ‘confirm’ or ‘determine’ the meaning of treaty provision being interpreted. It should be noted that arguably the use of Article 32 is not mandatory due to the use of the term ‘may’ rather than ‘shall’ as found in Article 31, therefore, conceivably Article 32 does not have to be resorted to even if Article 31 provides an ambiguous or absurd result. However, in practice it is difficult to foresee a time to take advantage of such a possibility in good faith, as reasonably the principle of good faith must include a genuine desire to determine the meaning of a provision rather than purposefully leaving it obscure or absurd for a favorable interpretation. Secondly, due to the denotation of Article 32 as the ‘supplementary’ means of interpretation and the wording explicitly requiring that Article 31 has produced an unsatisfactory result, it is clear that there is a hierarchical structure between the two articles, whereby Article 31 is always applied first and Article 32 only if necessary.

Consequently, in light of the above considerations it becomes possible to contextualize the position of the 2016 ICRC Commentary and its position in regard to the interpretation of Common Article 1. As it is a supplementary means of interpretation, for the Commentary to be relevant and considered in the process of interpretation, Article 31 must produce an ‘ambiguous’ or ‘absurd’ result. It can be feasibly argued that based on an interpretation in accordance with Article 31 based on the ordinary means of terms in the light of the objective and purpose of the treaty, the wording ‘ensure respect’ within Common Article 1 can be considered ambiguous.

This conclusion is primarily based on the lack of clarifying terms either before or after the contested wording, that is to say, while the first part of the sentence is clear ‘The High Contracting Parties undertake to respect’, which from an ordinary deconstruction conveys that the HCPs undertake an obligation to respect ‘the present Convention’. From this wording it can be derived that the HCP and everything it comprises of, take on the obligation to respect the Convention in all circumstances. However, when the terms ‘and to ensure respect’ for the Convention are added, suddenly it is arguably no longer clear where this obligation is directed. For if the obligation to ‘ensure respect’ was purely internal, the wording should include a clarification such as ‘and to ensure respect in the territory and population under its effective control’ for the Convention. Similarly, it can be argued that if the obligation’s external aspect

would have been emphasized a wording such as 'to ensure respect not only in its own territory and population but universally'. In either case, the scope of the latter obligation would have been confirmed. However, as this is not the case, arguably there is room to state that the meaning of the obligation to 'ensure respect' is ambiguous after an interpretation under Article 31 (1) and thereby warranting the use of supplementary means of interpretation under Article 32. Nevertheless, as will be discussed later in the following section 1.3, there are arguments for suggesting that the scope and meaning of the obligation 'to ensure respect' would be clarified under the subsequent practice and hence Article 31 (3) (b), however this is a contested interpretation.

Proceeding under the above presumption that there is sufficient ambiguity to interpret Common Article 1 under Article 32 of the VCLT, it must secondly be established that the 2016 ICRC Commentary is a relevant supplementary means of interpretation that can be used. The wording of Article 32 is not exhaustive in the sense that it offers a closed list of supplementary means of interpretation of preparatory materials and the circumstances of the treaty's conclusion. Rather that list is arguably non-exhaustive, as it is qualified by the term "including', thus conveying that while the following supplementary means are to be included in the possible supplementary means of interpretations, they do not represent all of them.

However, should every and any commentary be an acceptable supplementary mean of interpretation of equal worth, arguably that could create situation rife with potential for abuse, whereby either individual states or people write highly favorable commentaries on an international treaty. Through such biased commentaries states could attempt to import their own views into the international law being interpreted, thereby leading to a situation where there is no uniformity in the meaning of international treaty obligations. Such a situation would essentially void any benefit given by the principle of international law trumping domestic laws, at least for provisions that can be interpreted under Article 32.

Therefore, when assessing the 2016 ICRC Commentary, the special status of the ICRC must be considered[31]. The ICRC has been officially mandated by states to carry out its humanitarian mission and activities, with its mandate being incorporated in the 1949 Geneva Conventions as

[31] Debuf, E. (2015). Tools to do the Job: The ICRC's legal status, privileges and immunities. *International Review of the Red Cross,* Vol 97(897-898), 319-320.

well as their Additional Protocols and the Statutes of the International Red Cross and Red Crescent Movement[32]. One of these mandates is to promote and work for the faithful application of international humanitarian law[33]. Consequently, it can be soundly argued that for the faithful application of IHL the interpretation of said law must be clear, whereby conceivably one of the primary means of accomplishing that task is to provide commentaries on the relevant IHL instruments. Hence, any commentary provided on a relevant treaty that fits within that mandate will arguably have to be considered as a relevant supplementary means of interpretation for the purposes of Article 32 as the international community of states has entrusted such a mandate to the ICRC specifically.

As a result, as the 1949 Geneva Conventions are a cornerstone of IHL, the ICRC's Commentaries on them must therefore be recognized as a relevant and weighty supplementary means of interpretation for the purposes of Article 32. Thus, under the legal principle of *lex posterior derogat legi priori* whereby the later law prevails over an earlier law, the newer Commentary of 2016 should prevail over the older 1952 Commentary when addressing the same issue. Therefore, we may conclude that the 2016 Commentary is relevant for the purposes of interpreting the meaning of Common Article 1, and in terms of the hierarchy of commentaries should be considered to prevail over the older 1952 Commentary in cases of conflict.

1.3. Opposing Interpretations

There is debate regarding the scope of the obligation to 'ensure respect', whether it is narrow and not directed towards other parties, or broad and external as the updated 2016 ICRC commentary states[34]. In essence, to summarize briefly the debate, at the time of adoption the obligation to 'ensure respect' was not considered to be external in nature, as evidenced by the *travaux preparatoires*[35]. However, those in favor of a broad scope argue that since its adoption the

[32] Ibid., 320.
[33] Ibid., 321.
[34]Boutruche, T.,Sassoli, M. Expert Opinion on Third States' Obligation vis-à-vis IHL Violations under International Law, with a special focus on Common Article 1 to the 1949 Geneva Conventions' < https://www.nrc.no/resources/legal-opinions/third-states-obligations-vis-a-vis-ihl-violations-under-international-law/> accessed 21 February 2020.
[35] Breslin, A. (2017). Reflections on the Legal Obligation to Ensure Respect. *Journal of Conflict and Security law*, Vol. 22(1), 11.

meaning of the provision has evolved through subsequent practice to include an external dimension[36]. On the other hand, the counterarguments point to the existing contrary state practice and that Article 31 (3) (b) of the Vienna Convention on the Law of Treaties incorporates a high standard, which in their view the requires that all parties accept or acquiesce to the subsequent practice for it to be relevant[37].

Under the narrow view, the obligation contained in CA 1 to ensure respect pertains only to their organs and those acting under their effective control[38]. This has severe implications regarding AWS, as without the external dimension of the broad scope, it would be sufficient for HCPs to ensure that their own AWS respect the Convention. However, this obligation would nevertheless extend to supplied AWS in the sense that they should not encourage IHL violations on their own accord under CA 1[39]. However, should their supplied AWS be misused, CA 1 would not provide an obligation to ensure compliance by those systems, for the supplying state does not have effective control over them. Consequently, under the narrow scope the supplying states would only have to ensure that their own AWS and any AWS they have effective control over, respect the Convention and those supplied do not encourage violations.

Nevertheless, it ought to be highlighted that should a tether enabling effective control of a supplied AWS exist, then arguably it will be within the scope of the obligation to 'ensure respect' of CA 1 for the supplying state, even under the narrow view. However, the narrow view cannot require a supplying state to tether supplied AWS in the first place, as there is no obligation towards ensuring respect in regard to other states. Therefore, the design decision of whether supplied AWS are tethered will determine if CA 1 obligation will apply after they are exported. Thus, regardless of which interpretation prevails, CA 1's obligation to ensure respect will conceivably affect the design of AWS, for if a tether is included, then the supplying state must comply with that obligation even after the system has been supplied.

---

[36] Boutruche, T.,Sassoli, M. Expert Opinion on Third States' Obligation vis-à-vis IHL Violations under International Law, with a special focus on Common Article 1 to the 1949 Geneva Conventions' < https://www.nrc.no/resources/legal-opinions/third-states-obligations-vis-a-vis-ihl-violations-under-international-law/> accessed 21 February 2020, 7-8.
[37] Zych, T. (2009). The Scope of the Obligation to Respect and to Ensure Respect for International Humanitarian law. *Windsor Yearbook of Access to Justice*, Vol. 27, 256.
[38] Ibid., 270.
[39] Ibid., 265.

Nonetheless, for the purposes of this paper, from this point onwards, the obligation of 'ensuring respect' shall be construed to include an external dimension in accordance with the 'accepted' contemporary interpretation[40] in line with the ICRC 2016 Commentary as well as the Expert Opinion requested in the light of it[41]. This to enable the analysis of the relationship between CA 1 and AWS in its potentially most influential form, that is to say, whether it can require a tether to be included by the supplying state to all AWS they supply.

1.4. 'Reasonable' Means

The external duty to 'ensure respect' in regard to both preventing and bringing ongoing violations to an end, requires a HCP to do everything 'reasonably' in their capacity to meet that obligation, however, the meaning and limits of the term 'reasonably' are somewhat ambiguous. The 2016 Commentary offers some direction that aids in constructing a definition for 'reasonable' measures. Firstly, while the Commentary essentially gives freedom for states to choose the most appropriate measures[42], it explicitly clarifies that those measures must not contravene applicable rules of international law or by itself justify a threat or use of force contrary to Article 2(4) of the UN Charter[43]. Secondly, the Commentary requires that the gravity of the violations, the influence that HCP has over those responsible for the violation as well as the means 'reasonably' available to the state be considered[44].

Therefore, when considering the above, arguably the definition of 'reasonable' means must be derived in relation to the gravity of the breach and the degree of influence held over the violating party, all the while complying with other applicable international law. As a result, arguably the 'reasonable' means will increase with the severity of the breaches. Similarly, the more influential

---

[40] Breslin, A. (2017). Reflections on the Legal Obligation to Ensure Respect. *Journal of Conflict and Security law*, Vol. 22(1), 37.
[41] Boutruche, T.,Sassoli, M. Expert Opinion on Third States' Obligation vis-à-vis IHL Violations under International Law, with a special focus on Common Article 1 to the 1949 Geneva Conventions' < https://www.nrc.no/resources/legal-opinions/third-states-obligations-vis-a-vis-ihl-violations-under-international-law/> accessed 21 February 2020, 13.
[42] International Review of the Red Cross, *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 2nd edition*, 165.
[43] Ibid., 174.
[44] Ibid., 165.

the HCP is over the party committing violations, the more potential means will be considered 'reasonable' as a response to that situation.

When considering the interaction between AWS and 'reasonable' means to 'ensure respect' under Common Article 1 in light of the above, several possibilities can be considered. Firstly, provided the breaches are severe in nature, conceivably almost any course of action in relation to the AWS of the violating party, short of hijacking the systems and using force through them against the violating party are on the table. However, it is in this context important to determine what amounts to a 'use of force' within the meaning of Article 2(4) of the UN Charter, especially when considering whether the disabling of AWS through a remote tether can be considered to be a 'use of force'.

The term 'use of force' is not defined in the UN Charter itself, and as such it is no wonder that there is considerable debate regarding its exact meaning[45]. However, an important aspect of the definition is that elsewhere in the charter there are references to 'armed force' whereas in Article 2 (4) only the term 'force' is used, thus conceivably increasing the number of actions within its scope[46]. Therefore, if we consider that through the use of a tether, there would be three primary types of influences that the AWS could be subjected to, those being monitoring, full remote control and disabling, arguably each one would have to be separately examined to analyze if they would constitute 'force' under Article 2 (4).

Firstly, conceivably full remote control through a tether would be the most invasive of the three possibilities. Through such control the tethered AWS' behavior and actions could be directly controlled by the user of that tether, including committing IHL violations or 'friendly' fire incidents towards the state that the AWS supplied to. Consequently, full remote control has the highest possibility of constituting a 'use of force' under Article 2 (4) of the UN Charter, owing to its most invasive nature and possibility of using armed force against the state to which the system was supplied to. Hence, full remote control of the AWS through the tether would be the most difficult to justify as a 'reasonable method', for clearly merely a 'kill switch' for the system would equally prevent any future or ongoing IHL violations with a lesser degree of invasiveness.

[45] Haataja, S. (2017) 2007 Cyber Attacks against Estonia and international law on the use of force: an informational approach, Law, *Innovation and Technology*, Vol 9:2, 165.
[46] Ibid., 165.

Moreover, a purely 'on/off' tether would not provide the possibility of actually influencing the actions of the AWS, thereby reducing the possibility that if the tether was exploited by a third party the AWS could either commit IHL violations or 'friendly' fire incidents. Similarly, it would seemingly reduce the questions surrounding to whom or what should the actions of the AWS be attributed to, as there would at least not be a known vulnerability that would allow for remote control of the actions of the AWS. Obviously this would not eliminate the possibility of an unknown vulnerability being present and leading to the system being hijacked meaning the actions of that AWS would have to be attributed to hijacker rather than the state to which the system was supplied to. Nonetheless, it would mean that at least there was not an intentionally included vulnerability (i.e. the tether) that allows remote control, thereby making the prospect of remote control hinge on the presence of an unknown vulnerability being present which would constitute a more extraordinary circumstance.

Secondly, if we consider monitoring, it would appear to be the least effective solution in preventing at least ongoing violations while being almost as invasive as full remote control, which by definition would require some form of monitoring to be effective. For conceivably to remote control an AWS effectively it would be necessary to be able to 'see' what it sees to then decide on the best course of action, thereby necessarily including a monitoring aspect. Theoretically, an argument could be made that monitoring could prevent future violations if for example the intention to commit a violation is caught by the monitoring system or the orders that would result in a violation be noted by the AWS' monitoring tether. However, for that type of prevention to be a reasonable prospect, each and every supplied AWS would have to be continuously monitored by the supplying state, while effectively being able to spy on the military of the state to whom the system was supplied. Moreover, the actual possibility of preventing any action would rely in any case on the inclusion of either a 'kill switch' or a full remote control, therefore meaning that monitoring by itself cannot be used to 'ensure respect' for Common Article 1. Hence, it would appear difficult to justify why 'monitoring' would be a 'reasonable' means as it would likely have the least practical effect on preventing violations that are ongoing and only with great difficulty those that are about to committed, and essentially it would only benefit the supplying state as they would be able to effectively spy on the state to which the system was supplied to.

Therefore, only the possibility of merely disabling the AWS is left. By contrast it is the least invasive as it does not by definition necessitate monitoring or the capacity to influence the actions of the AWS beyond the possibility of disabling the system for future use. Moreover, it is effective in preventing both ongoing and future violations as that system would definitively not be able to be used for any purpose, including IHL violations. However, the sole inclusion of a disabling possibility through a tether without any monitoring is dependent on external information, i.e. the information about ongoing or future violations will have to be derived from other sources. This represents the primary relative weakness to both monitoring and remote control, as in both cases the AWS could be used as the source of information regarding the violations. However, considering that conceivably the violations would have to be severe and widespread to warrant the disabling of AWS in the first place, it would seem reasonable to conclude that information of such egregious violations could be obtained elsewhere. Thus, it is reasonable to conclude that solely including a possibility of disabling the AWS through a tether is the likeliest possible 'reasonable means' to 'ensure respect' within the meaning of Common Article 1 that would not violate the prohibition on use of force in Article (2) (4) of the UN Charter when compared to the other options.

Nevertheless, if we consider the case of remotely disabling AWS, then nonetheless arguably that is a 'cyber-attack' for the lack of a better term, for it is done remotely and without the consent of the state using the AWS. The question of exactly when and what type of cyber-attacks will be considered as a 'use of force' is hotly debated and there is a lack of binding international law on the matter, however, there are guiding instruments such as the Tallinn Manual that can be used for reference[47].

Rule 69 of the Tallinn Manual 2.0 provides a definition for when a cyber operation can be considered to be a 'use of force' within the meaning of the UN Charter[48]. Firstly, based on expert opinion there is no basis to categorically exclude cyber-attacks from being able to qualify as a use of force[49]. Secondly, the scale and effect have to be considered when considering whether a cyber operation will constitute a 'use of force'[50]. Thirdly, it is specifically mentioned that

[47] Ibid., 165.
[48] Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. (2nd ed) Cambridge: United Kingdom, Cambridge University Press, 330.
[49] Ibid., 331.
[50] Ibid.

economic coercion does not constitute a 'use of force'[51], which is somewhat indirectly mirrored in the 2016 Commentary whereby the suggested measures for ensuring respect include economic measures such as economic restrictions, refusing arms transfers and reduction of aid[52].

It may be tempting to state that disabling AWS remotely through a tether is merely the modern updated version of an arms embargo, however, as with other cases the use of analogies in relation to AWS and existing conventional concepts causes significant inaccuracies and oversights[53].For if we consider a traditional arms embargo, it is not capable of affecting the existing arms arsenal of the state being embargoed, but rather its effects are directed towards the prospect of its future replenishment. By contrast, the disabling of existing AWS of the violating state is by far more intrusive as it renders the existing systems useless thereby reducing the existing military strength of the state directly. Consequently, there is no conventional analogy, as such remote control arguably has never been possible before. As a result, it would be disingenuous to state that the disabling of AWS remotely would merely be an 'updated' arms embargo.

Indeed, if the situation is considered not in the context of a state violating IHL, but rather merely the supplying state disabling the AWS they have supplied for their own selfish purposes, it arguably becomes clear how such a measure could very well amount to a 'use of force'. Certainly, if we consider the criteria put forward by the Tallinn Manual 2.0 in assessing whether a cyber operation may constitute a use of force, such as severity, immediacy, directness, military character and state involvement, the remote disabling of AWS would fulfill several if not all of them. For example, the effects of disabling the AWS would be severe militarily as they cannot be used, as well as immediate and direct as the act of disabling them is directly related to its consequences of those systems being unable to be used. Similarly, as the AWS are military in nature, the military character of the situation is obvious, and as it is a state making the decision to disable the systems, state involvement is also present.

---

[51] Ibid.
[52] *International Review of the Red Cross, Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 2nd edition 181.
[53] Crootof, R. (2018). Autonomous Weapon Systems and the Limits of Analogy. *Harvard National Security Journal*, Vol 51, 83.

However, arguably the situation could be framed differently if the remote disabling is done due to the IHL violations of the state whose systems are being disabled. If it is agreed beforehand with the purchasing state, that the AWS supplied will be tethered to the supplying state, and that the tether may be activated under specific conditions such as grave breaches of IHL by that state. In this case, the situation would conceivably be quite different. Arguably, it would be difficult for the state whose systems have been disabled due to widespread IHL violations they themselves committed to argue that it was a 'use of force' against its military when they were aware of the conditions of use for the AWS that they violated.

In this vein, perhaps it is necessary to also shift our perspective on the weapons trade. That is to say, that weapon systems are no longer necessarily bought and sold in the traditional sense, but rather AWS can be bought and used conditionally. If we consider that until AWS, when a weapons system was bought and transported to its new owner, there was no way of influencing it short of damaging it through military action or sabotage. Under this old paradigm, the presumption therefore always was that the purchasing state is the 'absolute' owner of the system from that point forwards, and in theory, can use the system in any way it pleases without repercussions towards that particular system by the state from which it was bought.

Under the new paradigm with tethered AWS, the sale of weapons systems would involve an agreement or bilateral treaty that provides conditions for its legitimate use or else it will be subject to repercussions such as disabling. Therefore, if an AWS was bought under such a bilateral treaty or agreement and the purchasing state agreed to the conditions, then under the principle of *pacta sunt servanda*, that purchasing state could not later claim that the disabling of those systems was a 'use of force' against it when it knowingly violated the conditions of its use. With this new perspective and paradigm, arguably, the execution of such 'contractual penalties' in the form of disabling the AWS, should not qualify as a 'use of force', but rather a reasonable measure in the meaning of Common Article 1 to prevent and stop on-going violations.

Naturally, the weakness of this type of model would be the question of the standard of proof, not to mention attribution, regarding when those AWS could be disabled. For, arguably, the breaches would both have to be severe, attributable and evident for the disabling to be a reasonable measure. The issue of attribution especially when considering violations by AWS, which has already been noted to be potentially problematic in general, would likely be very significant. Furthermore, this difficulty is compounded by the difficulties in identifying the real sources of

cyber-attacks[54]. For it would have to be determined that the purchasing state was in fact responsible for the violation, and not that the violation was a result of the control through the tether by supplying state or faulty programming in the AWS. The latter situation would be problematic as one could argue that it could incentivize the purposeful inclusion of certain hidden faults that could then later be used as excuses to disable the AWS of the purchasing state. Similarly, as long as a tether exists that can influence the actions of the AWS beyond merely a binary on/off function, the argument could be made by the purchasing state that it was in fact the supplying state committing the violations through the remote control of the system.

However, in this vein it must be remembered that in a conflict it is not only AWS that are capable of violating IHL. Furthermore, it may be entirely plausible that a scenario might arise where the AWS themselves are not causing any violations of IHL, but the human troops used by a party to a conflict are responsible for widespread and severe violations. Provided that the AWS were provided under the proposed model of a bilateral treaty or agreement whereby their use is conditional to the state they are supplied to complying with their IHL obligations, arguably there is no need for the violations themselves to have been caused by those AWS specifically in order for them to be disabled. In such a situation, the disabling of that party's AWS systems, even if they are 'innocent', could be considered a 'reasonable' measure to ensure that the party committing the violations would refrain from causing further violations, owing to threat of an immediate reduction in their military strength due to disabled AWS.

In this type of a scenario the abovementioned questions relating to attribution of the AWS actions would not be relevant and the situation would be the same as it has been in the case of conventional human armies, thereby somewhat simplifying the questions of attribution. This in turn, may have the practical effect that in a future conflict the disabling of the AWS would likely be easier to justify by referring to the actions of the human combatants of that party, which unfortunately as a corollary implies that if a party wants to commit IHL violations, they should do them using their AWS owing to the more complex attribution process.

The mere existence of the possibility to blame the manufacturer of the AWS in this way could easily be transferred to a defense argument against the responsibility of the purchasing state in

[54] Sayapin, S., Tsybulenko, E. (2018). The Use of Force Against Ukraine and International Law: Jus Ad Bellum, Jus in Bello, Jus Post Bellum (1st ed), Hague: Netherlands, T.M.C. Asser Press, 218-219.

relation to the violations, whereby they claim that the system itself is at fault and by that extension its manufacturer. On the other hand, if the faults are so significant as to cause severe violations of IHL then conceivably it would be the duty of either party (the purchasing state or the producing state) to disable such affected systems to prevent future violations and thus 'ensure respect' within the meaning of Common Article 1.

Therefore, if such a contractual model would be adopted, there would have to be an independent body such as an arbitral tribunal created for that particular purpose to review whether the disabling would be justified. As such, arguably it is important to recognize that the disabling of AWS by the supplying state could be a 'use of force' if done for its own purposes and without a basis in an agreement or treaty with the purchasing state. However, if the disabling was done in accordance with a bilateral treaty or agreement with the purchasing state, conceivably it would not amount to a 'use of force' and thus could be a reasonable measure under Common Article 1 to address the breaches of IHL by the purchasing state.

1.5. Due Diligence

The external positive obligation of CA 1 to both prevent and bring violations to an end as well as bring the violating party back to an attitude of respect for the Conventions, confirmed in the 2016 Commentary is an obligation of means to be conducted with due diligence[55]. The term 'due diligence' in its general sense involves taking well-informed, prudent measures to avoid an undesirable outcome[56]. It should be noted that as recognized by the 2016 Commentary, that as it is an obligation of means, a HCP is not held responsible for a possible failure, provided it has done everything reasonably in their capacity to bring the violation to an end, i.e. acted with 'due diligence'[57]. It should be noted in the 2016 Commentary the duty explicitly includes not only stopping ongoing violations, but also an obligation to prevent foreseeable future violations[58].

[55] International Review of the Red Cross, *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 2nd edition 165.
[56] McDonald, N. (2019). The Role of Due Diligence In International Law. *International & Comparative Law Quarterly*, Vol 68 (4), 1041.
[57] International Review of the Red Cross, *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 2nd edition 165.
[58] Ibid., 164.

The 2016 Commentary affirmed the 'horizontal protection' aspect of the 'due diligence' in terms of the Law of Armed Conflict (LOAC), which has been contested in the past[59]. 'Horizontal protection' referring to the aspect that the protection is towards 'others' i.e. third persons including other states whose actions are not attributable to the state providing the horizontal protection[60]. The reasoning being that the concept of 'due diligence' is not applicable when the state itself through conduct attributable to itself causes the violation, as it is absurd to ask if the state has complied with its obligation to prevent a violation it actively participated in[61].

Therefore, the concept of 'due diligence' warrants protection against other parties such as other states[62]. In terms of contestation of this notion in the LOAC, the debate surrounded which actors constituted those 'other parties' i.e. if that included other states, which in essence mirrors the debate discussed in Section 1.3. of differing interpretations of CA 1[63]. Hence, in terms of the 2016 Commentary and CA 1, the applicable 'due diligence' concept can be considered to mirror the general definition in public international law as an obligation which requires a state to take all reasonable measures in its power to prevent and end violations by others, i.e. non state actors or other states[64].

Within the 2016 Commentary itself, the 'due diligence' obligation is stated to be similar to that which is found in Article 1 of the 1948 Genocide Convention, which provides for a state's obligation to employ all means reasonably available to them to prevent genocide[65]. Moreover, when assessing whether or not the state has complied with the standard of 'due diligence' factors such as the capacity to effectively influence the actions of person about to or committing the violation, the geographic distance and the strength of political and other links are to be assessed[66].

---

[59] Berkes, A. (2018). The Standard of 'Due Diligence' as a Result of Interchange between the Law of Armed Conflict and General International Law. *Journal of Conflict & Security Law*, Vol 23(3), 440.
[60] Ibid.
[61] Ibid.
[62] Ibid.
[63] Ibid., 441.
[64] Ibid., 433.
[65] International Review of the Red Cross, *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 2nd edition 166.
[66] Ibid.

The 2016 Commentary notes in particular that the duty to 'ensure respect' is particularly strong in regard to 'partners' such as those equipping, arming or training the armed forces of a party to a conflict, in which case they have a 'unique position' to influence the violating party and thus, to ensure respect for the Convention[67]. Therefore, when considering the above in light of AWS and having established in Section 1.4. that tethering enabling remote disabling of the systems can be considered to constitute 'reasonable means', provided it is technically feasible and reasonable, the question of whether complying with 'due diligence' could require such a tether arises.

As a tether could likely not be included after supplying, the decision to include a tether would therefore have to be done prior to handing over and supplying the system. Consequently, firstly to warrant a tether, the AWS would have to foreseeably have a risk of committing violations in the future. However, one could argue that even if the AWS or even just autonomous systems (including for example unarmed trucks) could not be used to commit IHL violations, a supplying state might still be required to include a tether to comply with due diligence to increase the leverage over the receiving state. As this additional leverage would 'ensure' that the receiving state would 'respect' the applicable rules as otherwise their systems would be disabled. Therefore, from a purely compliance perspective, arguably the supplying state would have done absolutely everything reasonably in their power to prevent future violations from occurring in the future. For even if the particular AWS that the supplying state supplied are not used in violations, the possibility of shutting down significant portions of the receiving state's military would arguably incentivize overall compliance, and hence serve to discourage committing of violations pre-emptively.

By contrast, a state that does not include a tether but could have reasonably done so, in light of the above considerations, could easily be viewed as not having done 'everything' in their power to prevent future violations. This negative perception of a supplying state not including tethers could conceivably be compounded by a perceived disregard for the 'unique position' of supplying states mentioned in the 2016 Commentary. Therefore, arguably a conceiving case could be made for warranting supplying states to include a tether capable of remotely disabling AWS on the basis of the 'due diligence' aspect of CA 1 to ensure an attitude of respect and prevent violations by the receiving state.

---

[67] Ibid., 167.

2. Autonomous Weapons Systems

2.1. Introduction to Autonomous Weapons Systems

Autonomous weapons systems are no longer contained within the realm of science fiction as already in the present day there are, for example missile-defense systems that can work entirely autonomously. These include the U.S. Aegis control system with the Phalanx Close in Weapons System (CIWS), that has a mode where it presumes the human operators are incapacitated and it can engage incoming missiles and aircraft on its own[68]. From this example we may derive the key aspects for defining an autonomous weapons system, a weapons system that is capable of independently identifying and making the decision to engage targets without human intervention, which mirrors for example the U.S: definition of an AWS closely[69]. Naturally there is much discussion regarding the precise definition, however for the purposes of this discussion, we will use the above definition whereby a weapons system is autonomous when it can identify, target and engage without human intervention.

The lack of human influence has led to discussions about the 'responsibility gap'[70] regarding the AWS, similar to the discussion about liability for self-driving cars and other vehicles. In both cases, the option that are most often discussed are that either the manufacturer and/or programmers are held liable, the seller, the operator, in limited cases the user (such as in the case of neglect that leads to a failure) or even the machine itself[71]. While each has their pros, cons and limitations, the discussion is too complex to attempt to solve in the context of this paper.

Nevertheless, a few aspects must be discussed in this regard. Firstly, the question of the possibility of human intervention is crucial for the accountability for the actions of the autonomous system. Arguably if a person has the possibility of influencing the autonomous system, it is not truly autonomous as that person will be held responsible for failing to prevent

[68] Crootof, R. (2018). Autonomous Weapon Systems and the Limits of Analogy. *Harvard National Security Journal*, Vol 51, 59.
[69] Bode, I., Huess H., (2018). Autonomous Weapons Systems and changing norms in international relations. *Review of International Studies*, Vol. 44, 399.
[70] Marcus Schulzke, 'Autonomous Weapons and Distributed Responsibility' (2013) *Philosophy & Technology 26*, 206.
[71] Hevelke, A., Nida-Rumelin, J. (2015). Responsibility for Crashes of Autonomous Vehicles: An Ethical Analysis. *Science & Engineering Ethics*, Vol.21(3), 620-621 & 623-624.

the system from malfunctioning. Hence, in the case of autonomous vehicles it is a complex legal and ethical question of whether such a possibility should even be included, as its inclusion would defeat the point of the autonomous vehicle, as a human would still have to supervise it, thereby removing the benefit of for example sleeping while travelling[72].

The same will hold true for AWS, except with the added dimension that now the autonomous system can make decisions to specifically end human life. Therefore, in the case of AWS the pressure to include such safeguards is increased, however, it raises further ethical questions, if the AWS is capable of operating unsupervised in a dangerous situation, is it ethical to endanger your own soldiers' life by placing them inside the system to monitor its operation? This desire to protect the lives of one's own soldiers has already provided the incentive for the development of robots used to defuse improvised explosive devices (IEDs) and other bombs[73], and as such it is reasonable to assume that the same desire will continue to incentivize the development of AWS.

Secondly, it may be an unfortunate reality that not all AWS can be monitored if they are on the offensive, as it may be beneficial from a military point of view that they abstain from unnecessary communications and are thus as 'radio-silent' as possible, to prevent their location and destruction by the enemy by means of tracking and tracing. The communication link between a modern unmanned weapons system are already noted as their weakest aspect[74], consequently, it would be reasonable to conclude that a purely AWS would address this weakness by being less reliant on communications to command and control. Hence, it is conceivable that future AWS may not have any human overrides, which would create the 'accountability gap'[75]. In the context of this discussion, it would mean that the supplying state, if they so desire, could distance themselves from supplied AWS in a similar way to 'traditional' weapons operated by humans, by stating they have possibility of influencing them.

However, a further aspect in relation to AWS that is closely related, is the unprecedented opportunity to include a pre-programmed 'basic moral code', whereby the AWS would simply

---

[72] Ibid., 619-630.
[73] Fleischman, F. (2015). Just say "no!" to lethal autonomous robotic weapons. *Journal of Information, Communication and Ethics in Society*. Vol 13(3/4), 302.
[74] Roff, H. (2014). The Strategic Robot Problem: Lethal Autonomous Weapons in War, *Journal of Military Ethics*, Vol. 13(3), 219.
[75] Schulzke, M. (2013). Autonomous Weapons and Distributed Responsibility, *Philosophy & Technology*, Vol. 26, 206.

refuse to comply with certain commands, such as those in clear violation of the Geneva Conventions. This situation is distinct from present reality where human combatants may harbor hidden 'characteristics' unknown to their commanders, such as hatred of certain ethnicities, a thirst for revenge in the heat of battle or hidden mental diseases[76]. The possible presence of these hidden characteristics in human combatants are preventable in AWS, where despite a potential capacity to learn and adapt, the programming of the system could nonetheless include safeguards like Asimov's laws of robotics[77] i.e. absolute prohibitions that underlie all operations.

Due to this possibility, the state supplying and producing AWS has a concrete and unique possibility to prevent those systems from violating IHL norms, and thus 'ensure respect' for the Geneva Conventions. Moreover, potentially the AWS could be used as a 'vigilance system' whereby the AWS observing violations of IHL would either store details of those violations in a black box type of storage or send them to either the manufacturer or another relevant entity, such as the Protecting Power(s) or even the ICRC. Similarly, the AWS could store all the orders it has received from its human operators in a similar log allowing for retroactive tracing of who gave the command and what the command exactly was, thus potentially identifying commands that were used to have the AWS commit violations of IHL. Moreover, if such features were to be included, non-physical safeguards should be considered as suggested in the Guiding Principles of a 2019 draft report by the Group of Governmental Experts for the CCW Convention, to prevent for example data spoofing that would reduce the utility of such a log and increase uncertainty related to its integrity[78]. Nonetheless, all these possibilities hinge on the producer of the AWS including or being required to include such features into their machines. Thereby giving further value in defining the obligations of CA 1, as arguably the above-mentioned possibilities, if they are technically feasible at the time, could certainly be included in measures reasonably in the power of the HCP supplying the AWS.

---

[76] Klincewicz, M. (2015). Autonomous Weapons Systems: the Frame Problem and Computer Security, *Journal of Military Ethics*, Vol. (14)(2), 164.
[77] Clarke, R. (1993). Asimov's laws of Robotics: implications for information technology. *Computer*, Vol. 26(12), 55.
[78] United Nations, 'Draft Report of the 2019 session of the Group of Governmental Experts on Emerging Technologies in the Area of lethal Autonomous Weapons Systems' <https://www.unog.ch/80256EDD006B8954/(httpAssets)/5497DF9B01E5D9CFC125845E00308E44/$file/CCW_GGE.1_2019_CRP.1_Rev2.pdf> accessed 17 April 2020.

Nonetheless, at the moment of writing, many discussions have taken place about legally regulating AWS as well as concerted efforts to outright ban AWS[79]. Including in the context of the UN Convention on Certain Conventional Weapons (CCW) in the form a pre-emptive ban such as in the case of blinding laser weapons, at present there are no international legally binding instruments on AWS[80]. Therefore, considering autonomous weapons are already in use to a degree, such as with the CIWS example and many research programs underway, it is safe to say the legal practice is lagging[81].

Arguably, from a practical standpoint it would be best not to hold one's breath waiting for a pre-emptive ban as arguably the benefits AWS bring are of such magnitude that the incentive to ban them may be somewhat limited by those capable of developing and fielding them. These advantages include political advantages such as reducing the threat of 'unpopular' wars as the casualties are not measured in lives but money, which arguably causes less opposition (especially if there is a strong economy to begin with)[82]. Meaning wars would impact the life of the average citizen less, provided it is not a 'fight for survival' but a conflict taking place at a distance from the state initiating the conflict, while the other side employs defensive fourth-generation military tactics in their land such as guerilla warfare we are accustomed to seeing in the 21st century[83]. Often taking the form of a major military power against a significantly weaker military, after which there is guerilla warfare for extended periods of time, such as seen in the Iraq and Afghanistan wars in the 2000s. As in the case of the Iraq war, mounting U.S. casualties increased the pressure to withdraw and increased criticism towards the war[84].

Several military advantage such as AWS systems needing no sleep and do not lose the ability to operate effectively over long periods of time (i.e. they do not get tired). Therefore, operations can be longer (provided supplies last) and take place during more trying conditions. In essence, AWS systems could be the 'perfect soldier', that needs no rest, has no fear and will fight as long

[79] Sharkey, A.J. (2018). Autonomous weapons systems, killer robots and human dignity. *Ethics and Information Technology*, Vol 21, 75.
[80] Bode, I., Huess, H. (2018). Autonomous Weapons Systems and changing norms in international relations. *Review of International Studies*, Vol. 44, 398-400.
[81] Ibid., 400.
[82] Asaro, P. (2012). On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making. *International Review of the Red Cross*, Vol 94, 692.
[83] Egeland, K. (2016). Lethal Autonomous Weapon Systems Under International Humanitarian Law. *Journal of International Law*, Vol. 85 (2), 98.
[84] Kriner, D., Shen, F. (2014). Responding to War on Capitol Hill: Battlefield Casualties, Congressional Response, and Public Support for the War in Iraq. *American Journal of Political Science*, Vol.58 (1),171-172.

as it is able to function. This means operations can be planned to be longer, more daring and so forth.

Logistics chains are simplified considerably, essentially only fuel, ammunition and spare parts need to be supplied. Meaning, water, food and medical supplies can be largely left out. This would mean significant improvements in the 'tooth-to-tail' ratio which would certainly go down significantly. For example, in 2005 28 % of the US Military in Iraq were combat troops and the rest were support personnel. Thus, this 'tooth-to-tail' ratio will be significantly reduced by AWS systems as they will require less support personnel, such as medical personnel, administrative personnel and logistics personnel to supply them. Moreover, if non-armed autonomous systems such as autonomous supply vehicles are introduced, the benefits even greater as even more support staff can be reduced.

As a corollary, this may result in an economic benefit, or at the very least a change in the overall cost of fighting a war. For, especially in the case of professional militaries, the less human soldiers are present, the less salaries have to be paid to them, not to mention their upkeep in terms of food and other essentials. Consequently, if through autonomation the amount of support (human) personnel could be reduced significantly, the cost of continuing to fight a war would arguably be reduced compared to the present, though on the other hand a more substantial initial cost might be expected which emanates from the cost of purchasing the autonomous systems. However, over time as those autonomous systems do not need to be paid a salary, the economic benefit over a traditional human military would materialize.

Therefore, when combined with the possibility of significantly reduced human casualties, the obstacles to fighting a long drawn out war would be considerably reduced, owing to the combined effect of the likely reduced economic impact over time of the war and the fewer casualties. This may reduce the effectiveness of guerilla war tactics considerably, as for the most part they rely on eventually draining both the economy and manpower of the invaders to eventually dissuade either the public or the military of the invading state that the invasion is no longer worthwhile or cannot be sustained. In light of the recent military conflicts that have seen even major military powers eventually forced to withdraw from their campaigns due to prolonged guerilla warfare, this potential newfound advantage through AWS against guerilla warfare is likely not to be discarded by those major military powers that need it the most.

Consequently, when assessing the potential advantages AWS may bring with them, from a practical point of view it would be prudent to ensure that as many legal questions surrounding them in the IHL framework are solved before they are introduced en-masse to the armed forces of states. If a pre-emptive ban does happen, the worst case scenario is wasted time, thoughts and effort in regard to the lawful use of AWS, whereas if the ban does not happen and AWS are introduced in a large scale manner, there could be significant loopholes in the application of IHL to the AWS.

2.2 Article 36 of Additional Protocol I

While legal practice can be said to be lagging in relation to the regulation of AWS, it must be recognized that the choice for the means and methods of warfare is not unlimited, which therefore includes the use of AWS[85]. The primary prohibition that must be adhered to in this regard is the prevention of using weapons that cause superfluous injury or unnecessary suffering[86]. AWS are hence subject to the same obligation by States to determine if a new weapon could be under any circumstances prohibited by the rules of IHL[87].

As a result, AWS are subject to Article 36 of Additional Protocol I (AP I) upon their 'development, acquisition or adoption' in those states that are party to AP I. Under Article 36 a HCP (to Additional Protocol I) is required to 'determine' whether the employment of a new weapons system would in certain or all circumstances 'be prohibited by this Protocol [AP I] or by any other rule of international law applicable to the High Contracting Party'. Consequently, an assessment will have to be made regarding the compliance of an AWS by both the exporting state during the study, development and adoption of it, as well as the receiving state during its acquisition and adoption, as it cannot merely rely on the manufacturer's or exporting State's assessment but must make its own[88].

[85] Van Den Boogaard, J. (2015). Proportionality and Autonomous Weapons Systems. *Journal of International Humanitarian Legal Studies*, Vol 6, 256.
[86] Ibid.
[87] Ibid.
[88] (2006). 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, *International Review of the Red Cross*, Vol. 88(864), 952.

However, there is a number of concerns regarding the effectiveness of Article 36 that may minimize its actual effect on AWS and their introduction. Firstly, there is the problem of classifying AWS owing to the multitude of forms they may take. For example, even in the seemingly simple case of a killer drone, the situation is far more complex than a surface level examination would indicate. A drone, at least a present, is an airframe with sensors that when produced does not have any weapons, and therefore not a weapon[89]. The drone only becomes a 'killer-drone' when it is coupled with armament, which would have been tested for compliance under Article 36[90]. Therefore, the exact status of this combination is arguably unclear, whether the resulting combination is a new weapon, method or means of warfare as included in the scope of Article 36. Moreover, the situation becomes likewise unclear if an existing weapons system (that has already been evaluated) is 'autonomised' i.e. made autonomous through the introduction of new software, as would be in the case of for example an existing anti-aircraft system being re-fitted with autonomous software that replaces the need for a human crew.

In either case, the importance of the scope of Article 36 will be of utmost importance, that is to say the meaning of the obligation to evaluate 'new weapon[s], means or method[s] of warfare'. If an existing weapons system is 'autonomised', arguably the existing physical weapons system will remain the same, but rather the 'brains' behind the weapons systems will no longer be biological, therefore, it is not a 'new weapon'. Consequently, for it to be within the scope of Article 36, it must therefore be either a "means" or "method" of warfare. The definition of these two terms is poorly understood, and it has been argued to not extend to the way the weapons are used, and that the article refers only to physical weapons, especially by those favoring a narrow interpretation of Article 36[91].

Hence, the problem of categorizing an autonomous system arises, is the autonomous control of a weapons system a weapon in itself or a way that a weapon is used that could be outside of the scope of Article 36. If the existing physical system is the same, is replacing humans with an autonomous software controlling the physical system, akin to an entirely new system that must be classified as such or a 'crew change' similar to swapping the individuals of the crew.

---

[89] Solis, G. (2016). *The Law of Armed Conflict: International Humanitarian Law in War.* (1st ed) Cambridge: United Kingdom, Cambridge University press, 550.
[90] Ibid.
[91] Rappert, B., Moyes, R., Crowe, A., Nash, T. (2012), The roles of civil society in the development of standards around new weapons and other technologies of warfare. *International Review of the Red Cross*, Vol. 94 (886), 782.

Conceivably, it would be possible to argue either way, for the situation could be represented as a change from a method of human warfare to robotic warfare. On the other hand, the argument could equally be made that as an existing weapons system does not have be re-evaluated every time the individuals making up the crew are changed, neither should this be the case for swapping that crew for an autonomous entity. Arguably, this question will remain until the meaning of the "means" and "methods" of warfare are definitively clarified for the purposes of Article 36.

Nevertheless, even when leaving out the questions of how the questions of autonomy fits into the framework of Article 36, there are more apparent and concrete issues with the scope of the obligation. Firstly, Article 36 is attached to Additional Protocol I, which means that it is applicable only to those states that have agreed to be bound by it, meaning that a number of significant military powers that are not known to conduct military weapons reviews such as Turkey, Iran and India are outside its scope[92]. Furthermore, it must be mentioned that states not formally bound by AP I such as United States and Israel, are known to carry out systematic weapons reviews, however, as they are formally not bound, the requirements of those reviews are not necessarily dictated by Article 36[93]. Therefore, it can be stated that Article 36 may not have a significant impact on the development of AWS at all, as numerous significant military powers are outside of its reach.

Secondly, as confirmed by the 1987 Commentary, the reviews conducted in accordance with Article 36 are not required to be publicized and thus can be subject to secrecy[94] adding to the lack of public material on weapons being developed[95]. This lack of transparency can no doubt compromise the effectiveness of the reviews conducted on new weapons systems, including those of an autonomous nature for there is a lack of international oversight[96]. Furthermore, this lack of transparency has already manifested in a number of states not conducting weapons

[92] Jevglevskaja, N. (2018). Weapons Review Obligation under Customary International Law. *U.S. Naval War College International Law Studies*,Vol 94, 191.
[93] Jevglevskaja, N. (2018). Weapons Review Obligation under Customary International Law. U*.S. Naval War College International Law Studies*,Vol 94, 209.
[94] 1987 Commentary 1470-148.
[95] Backstrom, A., Henderson, I., (2012). New Capabilities in warfare: an overview of contemporary technological developments and the associated legal and engineering issues in Article 36 weapons reviews. *International Review of the Red Cross*, Vol 94(886), 487.
[96] Rappert, B., Moyes, R., Crowe, A., Nash, T. (2012), The roles of civil society in the development of standards around new weapons and other technologies of warfare. *International Review of the Red Cross*, Vol. 94 (886), 781

reviews or seemingly relying on the review processes of larger military powers contrary to the requirements of Article 36[97]. Therefore, in combination with the substantial military advantages of AWS as outlined in Section 2.1., it would seem highly unlikely that Article 36 would prevent the introduction of AWS, especially as numerous significant military powers are simply not bound by it.

On the other hand, it has been argued that even if a state is not a party to AP I, it nonetheless has an obligation to conduct a weapons review on new weapon systems on the basis of customary law[98]. Unlike the usual arguments to prove the existence of a customary rule of international humanitarian law, the argument is not based on the consistent and widespread state practice and positive *opinion juris*, but rather the duty to comply with the law of armed conflict and the fundamental principles on which weapons reviews are based[99]. Those principles being the aforementioned prohibition on using weapons that cause superfluous injury, unnecessary suffering and indiscriminate weapons[100].

However, in this context it must be mentioned that as noted above, the AWS may not actually represent new weapons in the true sense of the term, that is to say, they will use existing 'conventional' missiles, small arms and cannons. Rather the only difference could be reduced to the fact that now the 'brain' controlling their use is now artificial rather than biological. Therefore, if a weapon did not cause superfluous injuries or unnecessary suffering, conceivably it would not do so in the future either merely because it is now autonomous.

On the other hand, a more credible case could be made that a previously accepted weapons system could be considered indiscriminate when it is controlled by an AWS. This would require that the AWS is incapable of discriminating between legitimate and illegitimate targets and therefore that weapons system could not be directed at a specific military objective. However, already from the point of view of the state deploying such a weapon one would have to question the rationality of deploying such a system, as such a system is unlikely to produce an appreciable military advantage if its capacity to identify targets is so seriously compromised. Nonetheless, it

[97] Ibid.
[98] Jevglevskaja, N. (2018). Weapons Review Obligation under Customary International Law. *U.S. Naval War College International Law Studies*,Vol 94, 188.
[99] Ibid.
[100] Ibid.

would not be an inconceivable scenario that a specific AWS could not be used due to its indiscriminate nature, however, arguably that restriction would not be applicable to all AWS, but rather specific to that system in particular. For as long as an AWS is capable of discriminating between legitimate targets, its use would likely be legitimate, provided the conventional weapons it is paired with are equally legitimate.

While the debate regarding the existence of a customary law rule for a weapons review continues, the mere existence of those fundamental principles would logically suggest that in order to determine if a weapons system violates them, it would have to be reviewed or evaluated beforehand[101]. However, the practical effects have been less encouraging[102]. In fact, if the case of the blinding laser weapons is evaluated, while it may obvious now that they case superfluous injury and/or unnecessary suffering, it took Protocol IV to the CCW for such laser weapon development programs to be halted[103]. Consequently, the actual persuasiveness of the fundamental principles and the duty to comply with the LOAC absent a specific instrument can certainly be questioned in this light. Therefore, arguably when considering the above, neither Rule 36 of AP I nor any customary rule of international humanitarian law can be considered to likely result in a uniform ban on AWS.

Hence, when considering the less influential and somewhat arguably ineffective Article 36 of Additional Protocol I and the dubious existence of a customary law rule, the universally applicable Geneva Conventions including Common Article 1 represent the most widespread possibility of influencing the design and use of AWS in the future. Consequently, the importance of interpreting the contents of the Geneva Conventions, such as that of Common Article 1 in relation to AWS is of utmost importance.

[101] Ibid., 218.
[102] Ibid., 218-219.
[103] Ibid., 219.

3. Interaction of AWS and Common Article 1

3.1. Not all AWS are created equal

Autonomous weapons systems are not mentioned in the 2016 Commentary, nor how would the obligations of the Article interact with them. Nonetheless, based on the discussion in the previous sections about the nature of AWS, as they can make decisions to engage targets on their own, it is foreseeable that they could do so in violation of IHL norms. Therefore, the positive obligation of preventing violations when there is a foreseeable risk[108], would apply to such AWS systems.

This presumes that the AWS systems in question can cause harm or use lethal force, meaning that a distinction must be made between AWS systems where it is foreseeable that they may cause violations from those that foreseeably could not. It is reasonable to presume that the armed forces will adopt (unarmed) autonomous vehicles such as cars and trucks, but arguably as they are not designed to have a combat role, they are unlikely to cause violations of IHL in their normal operations. By contrast, the moment an autonomous vehicle is armed, the situation becomes different as foreseeably the armament could be misused

However, the distinction may be even more difficult if we consider the present example of the already autonomous Goalkeeper CIWS system that can engage missiles and aircraft on its own. First, we must consider it is a mounted system that is immobile, whereby its operation can be closely monitored by humans, even if they do not contribute to the decision-making of the system and hence the system shut down if it malfunctions. Secondly, the system is designed to engage high-speed targets such as missiles and aircraft with the capacity to identify friend or foe (IFF functionality), meaning it can distinguish between civilian and military aircraft[109]. Thirdly, the system is short ranged (2000 meters)[110], which in combination of only targeting high-speed objects such as missiles, and its ability to distinguish civilian aircraft, would mean that the

[108] International Review of the Red Cross, *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 2nd edition, (2016), 164.
[109] Seaforces, 'Goalkeeper close-in weapon systems' <http://www.seaforces.org/wpnsys/SURFACE/Goalkeeper-CIWS.htm> accessed 23 December 2019.
[110] Ibid.

foreseeable violations would be limited to engaging a misidentified civilian aircraft that stray within 2000 meters of the system. Considering the specification of the above system, despite it being a lethal AWS, as it is capable of destroying aircraft, it is difficult to identify many foreseeable risks in terms of IHL violations as it is highly unlikely to actually interact with protected persons under the Geneva Convention and as outlined above could violate IHL in highly specific scenarios only.

By comparison, a mobile airborne autonomous drone engaging in a persistent campaign of targeted killings[111] would be at a higher risk of foreseeably causing IHL violations as it can target a variety of ground forces, installations as well as potentially civilian targets. Consequently, the foreseeable violations of IHL that the system is capable of causing is far wider than in the case of an autonomous CIWS system.

Both systems in the above examples can be exposed to cyber threats as they rely on and operated by computer systems. Hence, it is plausible to consider a scenario, where a cyberattack causes the AWS to violate IHL[112]. Although currently there is no obligation on states to foresee and analyze possible misuses of weapons[113], it may be argued that given the relative, but inherent insecurity of computer systems, it can be reasonably expected that tampering by cyber means will, sooner or later, take place and can affect the normal and expected use of an otherwise legal AWS. Nevertheless, while no such binding obligation exists, the topic of cyber security in AWS in the context of non-physical safeguards has been mentioned in the Guiding Principles of a 2019 draft report by the GGE for the CCW Convention as an aspect to consider, thereby suggesting at the very least mounting discussions on the topic that could eventually lead to binding obligations in the future[114]. Potential misuse of AWS by adversaries via exploiting unknown vulnerabilities and resulting the risk of violations of IHL are hardly foreseeable in advance. However, the same

---

[111] Carl Haas, M., Fischer, SC. (2017). Evolution of targeted killing practices: autonomous weapons, future conflict and international order. *Contemporary Security Policy*, Vol. 38(2), 283.
[112] Schmitt, M., (2013). Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics. *Harvard National Security Journal Features*, 7.
[113] ICRC Commentary on the Additional Protocols, paragraph 1469. Also see Michael N. Schmitt (ed) Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations, 466.
[114] United Nations, 'Draft Report of the 2019 session of the Group of Governmental Experts on Emerging Technologies in the Area of lethal Autonomous Weapons Systems' <https://www.unog.ch/80256EDD006B8954/(httpAssets)/5497DF9B01E5D9CFC125845E00308E44/$file/CCW_GGE.1_2019_CRP.1_Rev2.pdf> accessed 17 April 2020.

cannot be said about already known vulnerabilities. Therefore, although analysis of misuses may not be required as such under IHL or other international law obligations, it is nevertheless questionable whether the existence of a known vulnerability in an AWS that can potentially lead to violation of IHL, would render the risk of that violation foreseeable.

Consequently, the foreseeable risk of violations is highly specific on the type of AWS, and as such AWS cannot be categorized merely based on their autonomous function or potential lethality, but rather a system-by-system overall risk analysis must be performed. Consequently, a state supplying a system like the Goalkeeper CIWS, they would arguably have to take fewer preventive steps to inhibit the system from causing IHL violations when compared to a state supplying an autonomous 'killer-drone'. As such, the actual content of the obligations under CA 1 would be different based on the types of AWS supplied, and in that sense the obligations cannot be mapped out precisely in the abstract. However, it is possible to state abstractly that the HCP should take all measures in ensuring the AWS cannot cause the foreseeable violations of IHL specific to that system. Such measures should include a misuse risk assessment by identifying and appropriately addressing at least known cyber vulnerabilities that can lead to violations of IHL.

3.2. The External Positive Obligation of Common Article 1

Under Common Article 1, the HCPs have the positive obligation of both preventing future violations as well as stopping ongoing violations by a party to a conflict. Consequently, as the AWS provide the unprecedent opportunity to definitively pre-program a set of rules that the physical weapons system must follow, such as to prevent violations of IHL. Of course, considering the complexity of both practical situations in a conflict as well as the legal framework, the correct course of action can be difficult to determine. As such, there has been doubt expressed whether AWS can ever operate within the correct manner from an IHL point of view[115]. However, arguably that is dependent on the type of system as outlined above in 3.1.

[115] van Kralingen, M. (2016). Use of Weapons: Should We Ban the Development of Autonomous Weapons Systems?. *The International Journal of Intelligence, Security and Public Affairs*, Vol 18:2, 137.

Nonetheless, it would be a gross oversimplification to reduce the situation to programming the system with a simple set of rules such as 'never target non-military infrastructure' or 'never cause the death of a civilian' to definitively prevent violations. While both are in theory protected, in practice the situation may be more complicated and would not necessarily involve a violation of IHL, depending on the proportionality and the military advantage gained. The exact weight of each factor in the equation of military advantage gained versus collateral damage remains controversial[116], and therefore quantifying it for an autonomous system equally problematic[117]. Moreover, the proportionality assessment is based on the expected outcomes, that is to say an attack should only be carried out when the expected 'cost-benefit' of that attack is determined to result in more of a military advantage than the costs to humanity and incidental civilian damage[118]. As a result, a proportionality assessment will require predictive and abstract thinking from the entity which conducts it, hence it will not be sufficient that an AWS is able to merely identify the immediate effects of the attack, but also the long-term repercussions.

For example, a bridge can be entirely a civilian structure, however, the military advantage of destroying said bridge, may justify the destruction of the bridge and thus abstractly 'transforming' it from a civilian to a military target[119]. However, a proper assessment for the destruction of the bridge should consider the long-term effects on the civilian populace, highlighting the necessity for predictive and long-term reasoning for an AWS. Similarly, in the case of a targeted killing campaign, if a high-ranking enemy is found, who however is in the presence of a civilian and a decision to engage would end both of their lives, conceivably considerations of military advantage and proportionality could justify the killing of the civilian alongside the high-ranking commander [120].

Thus, both cases highlight that commands that appear almost like a tautology such as 'never kill or cause the death of a civilian' are not always a realistic possibility to include as 'overruling'

---

[116] Wells-Greco, M. (2010). Operation 'Cast Lead': Jus in Bello Proportionality, *Netherlands International Law Review*, Vol. 57 (03), 400.
[117] Grut, C. (2013). The Challenge of Autonomous Lethal Robotics to International Humanitarian Law. *Journal of Conflict & Security Law*, Vol 18(1), 13.
[118] Horvitz, A., Nehs, R. (2011). Proportionality and international humanitarian law: an economic analysis. *Global Change, Peace & Security*, Vol. 23(2), 206.
[119] ICRC, 'Practice Relating to Rule 10. Civilian Objects' Loss of Protection from Attack' <https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule10> accessed 23 December 2019.
[120] ICRC, 'Practice Relating to Rule 14. Proportionality in Attack' <https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule14> accessed 23 December 2019.

laws in a manner similar to Asimov's laws of robotics. Consequently, the task of pre-programming an AWS to such an extent that under absolutely no circumstances it could violate IHL, arguably is a herculean task. Consequently, the supplier of an AWS, likely could never eliminate the chance of their AWS causing violations purely based on its programming. Of course, if such a technological feat is possible, feasibly CA 1 would require that the supplied AWS would be included with such programming as it would be a measure reasonably in the power of the supplying state. However, in this regard we must be realistic and assume it is not possible, at least for all systems, for the near future.

Therefore, from the above conclusion we arrive at the second possibility that could potentially be required under CA 1, the question of whether or not the supplying HCP has the obligation to retain the possibility of influencing the AWS or monitoring its activity?

3.3 To Tether or Not to Tether?

The possibility of influencing the actions and behavior of AWS by means of remote-control raises the possibility of HCPs meeting the positive obligation of CA 1 of stopping or preventing IHL violations by taking control of their supplied AWS. This question is similar to that which has been taking place regarding encryption where there is a question of should backdoors be provided to give authorities access[121]. Naturally, in the case of AWS the discussion will have the added life-and-death dimension, whereby if a 'backdoor' is included and the system is hacked, lives could be lost in a dramatic and immediate manner. Moreover, the presence of a backdoor increases the amount of actors potentially able to commit IHL violations with the AWS, should a third party be able to hijack the system by exploiting the backdoor. On the other hand, to a degree this risk could be somewhat reduced by limiting the backdoors to only disabling the AWS, which if breached would not at least cause violations, but would hamper the utility of the AWS considerably.

[121] Rivest, R. (1998). Case against regulating encryption technology. *Scientific American*, 116-117.

However, arguably, there is no better or more immediate way of preventing violations by AWS used by a party to a conflict, than remotely disabling those system being misused. Therefore, in terms of purely a compliance perspective, the ability to remotely disable AWS would be ideal to ensure the respect for the Geneva Convention and other applicable IHL, even if it is somewhat a double-edged sword due to risk of unauthorized access. On the other hand, there are several other considerations that should be considered when determining whether tethering the AWS should be required as a means of fulfilling the obligations under CA 1.

First, let's consider the 'untethered' model whereby the supplying state severs or does not include to begin with, all possibilities of influencing the supplied systems once they have been supplied to another state. Thus, the supplying state would be entirely unable to monitor or direct their activities in the future. As a result, this would render AWS akin to 'traditional' human operated weapons systems in the sense that the supplier has no control over how they are used after handing them over. Consequently, the supplying state would have to resort to the 'traditional' means of influencing such as by exerting diplomatic pressure, economic sanctions and refusing to supply the conflict party in the future[122].

Under this untethered model, the introduction of AWS changes less in how the HCPs comply with the obligation to 'ensure respect' under CA 1. The only meaningful improvement would be the programming of the AWS aimed at preventing the misuse of the AWS when designing and supplying such systems. For arguably, that is included under the measures HCPs can reasonably take to prevent foreseeable violations. As discussed above in section 3.2 this would likely not cover all possible situations where violations can occur, and hence would likely not be a definitive panacea. Nonetheless, when compare to the present where the compliance or non-compliance of weapon systems is entirely at the mercy of their crews, it would conceivably still be an improvement.

[122] Dormann, K., Serralvo, J. (2014). Common Article 1 to the Geneva Convention and the obligation to prevent international humanitarian law violations. *International Review of the Red Cross*, Vol.96(895-896), 725-726; International Review of the Red Cross. (2016). *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 2nd edition, 181.

The second possibility is the 'tethered' model, which could be described by analogy as a 'Swiss mercenary of old' model. For if the supplying state maintains some form of connection, be it the capacity to monitor the activity, direct the activity or a remote 'kill-switch' for the AWS, the AWS is not truly an asset of the state it has been supplied to, but rather somewhat of a 'cyber mercenary'. Therefore, the analogy of considering the tethered AWS similar to the 'Swiss mercenaries of old', the use of which came with conditions in regard to their state of origin (Switzerland) such as that they may be recalled if the Swiss confederacy would come under attack[123]. Consequently, a prudent user of the Swiss mercenaries would have understood that they cannot be relied on, in all circumstances. Similarly, if the AWS would be tethered to their state of origin, those AWS would be transformed into a 'cyber mercenary' equivalent of this model, that could not necessarily be relied on, in all circumstances, be those circumstances when those AWS are used to cause violations of IHL, or conflict with the supplying state. Especially if there is a conflict with the state supplying the AWS, the user of those AWS may find that those systems have 'turned traitor', adding a whole new level to cyber warfare, and as such put them at a great military disadvantage.

That is to say, it can never be 'fully trusted' as similar to a Swiss mercenary of old, whereby, while they are entirely under the command of the local armed forces, they will nonetheless have a link to their state of origin. Similarly, tethered AWS will have a remote cyber link to the supplying state, which may be activated at any time, thus transforming them into a 'cyber mercenary' from the supplying state. Therefore, the armed forces of a state buying AWS might be compromised by the presence of these 'cyber mercenaries' amidst their ranks which may enable the supplier of those AWS to retain both political and military leverage over the state using those systems.

Naturally, this analogy is restricted by the use of the term "mercenary" as there is a risk of confusion with the terms present legal meaning under which a "mercenary" does not retain any link to its state of origin[124]. This use of inaccurate labels can create problems[125] and lead to

[123] McCormack, J., (1993). One Million Mercenaries: Swiss Soldiers in the Armies of the World. Barnsley: United Kingdom: *Pen and Sword Books*, 62.
[124] eg United Nations Mercenary Convention Article 1 (1) (e) and 1 (2) (d)
[125] Tsybulenko E., Francis J.A. (2018) Separatists or Russian Troops and Local Collaborators? Russian Aggression in Ukraine: The Problem of Definitions. In: Sayapin S., Tsybulenko E. (eds) The Use of Force against Ukraine and International Law. T.M.C. Asser Press/Springer, The Hague, 139-140.

attempts to justify positions in regard to international law with those inaccurate labels[126] when further considering this model, even if it is the closest existing analogy. Consequently, this "cyber mercenary" that is analogous to a Swiss mercenary of old, would arguably require a new term without pre-existing definitions or prejudices. In this vein, a portmanteau between 'autonomous' and 'mercenary' could be used, such as 'autocenary', which could be defined as "an autonomous weapons system that is tethered to its state of origin or production by means that enable disabling, monitoring or remote control'. Nevertheless, despite its limitations, the term 'cyber mercenary' will be used for the purposes of this paper.

Nevertheless, the tethering of AWS to the supplying state would solve one of the key questions of supplying weapons, what if they are ever used against the supplier? For on the one hand, the supplier wants to supply inferior systems so that they cannot compete with their own, but at the same time they must be better than the competing systems so that they are chosen over their competitors. Maintaining control would give the best of both worlds to the supplier, the systems can be as effective as possible, as the supplier knows that if ever they will be used against them, it is possible to disable or control them. Similarly, merely being able to monitor their use would allow the supplier to spy on the supplied state's armed forces, and as such gain valuable intelligence.

Moreover, if we accept that only the major military powers will be able to produce and develop their own AWS, tethering them to the supplier would multiply their leverage over the states that are forced to purchase foreign systems. Thus, leaving them with an 'unreliable' military full of 'cyber mercenaries' when compared to the major military powers who use their own systems. The leverage gained by such a tether, is conceivably both military and political, as not only does the supplying state have a measure of control over the military of the supplied state, but also political capital. For the aforementioned control could be used to ensure "favorable relations" with the supplying state by exploiting that leverage given by the tethered AWS.

However, it must equally be remembered that if the supplier is able to remotely access the AWS, conceivably so could a third party, thus the presence of tethering will additionally increase the vulnerability of the systems to cyber-attacks by third parties. This threat is especially

[126] Tsybulenko, E.; Platonova, A. (2019). Violations of Freedom of Expression and Freedom of Religion by the Russian Federation as the Occupying Power in Crimea. In: Baltic Journal of European Studies, 9 (3 (28)), 136.

elevated by the fact that if such a tether is required by law, third party actors will know that it must be present, therefore justifying a significant investment into attempting to exploit such a tether and the leverage over the military of the supplied state brought with it. By comparison, if no tether is required, third party actors would have to consider if such a tether even exists, and thereby the incentive to invest significant resources into exploiting a potential tether would be reduced due to the uncertainty.

As a result, while tethering the systems to the supplying state might appear the most tempting option to fulfill the positive external obligation under CA 1, if such a tethering was to be required by CA 1, then it would have significant arguably undesirable consequences for any state purchasing such systems. Therefore, it would be prudent not to be naïve when the tethered model is being advocated under the guise of added or assured compliance with the obligations of both IHL and especially, CA 1. Nonetheless, it must also be considered that it is equally possible that hidden backdoors and overrides can never be conclusively eliminated anyway, regardless of whether or not this would be required by CA 1, as the potential leverage is arguable tempting.

Conclusion

The relationship of the positive external obligation of Common Article 1 and AWS can take on a variety of directions, however arguably the key factor of the relationship is the question of tethering the supplied AWS so that the supplying state can 'ensure respect' as required by CA 1 in all circumstances. Certainly from a legal point of view, a compelling case can be made for requiring such tethering based on the need for HCPs to do 'everything reasonably in their power to prevent and bring such [IHL] violations to an end'[128] under the positive obligation of CA 1. For a tether that makes it possible to disable the supplied AWS would be an effective solution to preventing ongoing violations as well as both directly and indirectly preventing future violations by a party to a conflict. In terms of future violations, besides direct prevention by disabling the AWS, the tether would indirectly provide leverage by the mere possibility of switching off supplied AWS, and thereby reducing the military strength of supplied state immediately, which would likely 'encourage' them to maintain an attitude of respect towards their IHL obligations.

Furthermore, under the 2016 Commentary the means of accomplishing the positive external obligation of CA 1 is limited by applicable rules of international law including the prohibition of a 'use of force' within the meaning of Article 2 (4) of the UN Charter[129]. A convincing argument can be made that if a bilateral treaty or other agreement is made during the sale of AWS which stipulates that the use of the supplied AWS is conditional upon compliance with applicable IHL norms and if this condition is violated the tether can be used to disable the supplied systems. Therefore, subsequent use of the tether to disable the AWS that conforms with the agreement would not amount to a prohibited 'use of force' under Article 2 (4) of the UN Charter. Moreover, as opposed to full remote control or monitoring, the inclusion of only a 'kill switch' would comparatively be both the least invasive and most effective measure that could prevent both ongoing and future violations, and thereby the most reasonable. Thus, if the tether would only allow for disabling without the possibility of actual remote control or other forms of monitoring, arguably it can be considered to be a 'reasonable' mean in the power of the supplying state within the meaning of CA 1.

---

[128] International Review of the Red Cross. (2016). *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*. 2nd edition, 154.
[129] Ibid., 174.

Consequently, provided such a tether is technically feasible, it would be within the reasonable power of the supplying state to include such a backdoor for access, and would significantly aid in preventing both future violations as well as on-going violations. Hence, from a purely legal and compliance point of view, the inclusion of a tether could conceivably be justified by referring to CA 1's positive external obligation to 'ensure respect'.

The choice, however, in reality is more difficult and complex, as the trade-off is either potentially sacrificing compliance by not requiring the tethering, or by potentially compromising the armed forces of the supplied states with these autonomous 'cyber mercenaries' (autocenaries) in their ranks in exchange for added compliance. Moreover, the presence of tethering could significantly increase the risk of the AWS being interfered with or even hijacked by a third party, thereby further adding to the cyber security concerns of the systems. Moreover, requiring the tethering of the AWS could have significant political and military implications by further increasing the power of the states supplying AWS by providing them the opportunity to exploit the tether for their own purposes. Therefore, the political and military concerns of states who would be dependent upon supplied AWS should not be ignored as they would become increasingly disadvantaged militarily and politically dependent upon the states supplying them AWS. As a result, the AWS tethering question has to be examined beyond the purely legal perspective, taking into account the full-range of its potential effects on not only IHL compliance, but additionally the international *status quo*.

Moreover, it must be kept in mind that not all AWS are the same and involve similar foreseeable risks of committing violations of IHL. Therefore, arguably the question of 'to tether or not to tether' could be broken down to a case-by-case basis, whereby for example an AWS that has a relatively low-risk of causing violations, such as a stationary missile defense system, would not be under a tethering requirement, but a higher-risk 'killer-drone' could be. Under such a system-by-system model however, the legitimate concern can be raised that if one state supplies both tethered and untethered AWS, the receiving state will likely have trouble attempting to silence the doubt that on the 'untethered' systems, the tethers are merely hidden. Consequently, further discussions and contemplations are required on the matter, for conceivably at present the positive obligation of CA 1 could be used to justify such a 'tethered' system as it would ensure a higher degree of compliance and respect for the Geneva Conventions and other applicable IHL, though with significant political and military side-effects.

Nevertheless, the positive external obligation of CA 1 arguably has implications for the use and development of AWS and the states supplying them. The identified primary key issue arising from the relationship between CA 1 and AWS being the question of the tethering of AWS to the state of origin. However, as AWS can take a variety of different forms with different risk profiles, it is difficult to provide a conclusive all-encompassing answer as to whether the tethering would be appropriate in every case. This uncertainty is compounded by the additional political and military ramifications of tethering, as it would likely result in an increased power imbalance between the state using the AWS and the supplying state. Therefore, in conclusion, the positive external obligation of CA 1 has serious implications for AWS in potentially requiring tethering to the supplying state, a question which is best approached on a system-by-system basis owing to the diversity of AWS and their differing risk profiles.

List of References

Scientific Books

1. Alston, P., Steiner, H., Goodman, R. (2008). *International Human Rights in Context*. (3rd ed) Oxford: United Kingdom, Oxford University Press.

2. Clapham, A., Gaeta, P., Sassoli, M., (2015). *The 1949 Geneva Conventions: A Commentary*. (1st ed.) Oxford: United Kingdom: Oxford University Press.

3. Sayapin, S., Tsybulenko, E. (2018). *The Use of Force Against Ukraine and International Law: Jus Ad Bellum, Jus in Bello, Jus Post Bellum* (1st ed), Hague: Netherlands, T.M.C. Asser Press.

4. Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* (2nd ed) Cambridge: United Kingdom, Cambridge University Press.

5. Solis, G. (2016). *The Law of Armed Conflict: International Humanitarian Law in War.* (1st ed) Cambridge: United Kingdom, Cambridge University press.

Scientific Articles

6. Asaro, P. (2012). On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making. *International Review of the Red Cross,* Vol. 94(886), 687-709.

7. Backstrom, A., Henderson, I., (2012). New Capabilities in warfare: an overview of contemporary technological developments and the associated legal and engineering issues in Article 36 weapons reviews. *International Review of the Red Cross*, Vol 94(886), 483-514.

8. Berkes, A. (2018). The Standard of 'Due Diligence' as a Result of Interchange between the Law of Armed Conflict and General International Law. *Journal of Conflict & Security Law*, Vol 23(3), 433-460.

9. Bode, I., Huess, H. (2018). Autonomous Weapons Systems and changing norms in international relations. *Review of International Studies,* Vol. 44, 393-413.

10. Breslin, A. (2017). Reflections on the Legal Obligation to Ensure Respect. *Journal of Conflict and Security law,* Vol. 22(1), 5-37.

11. Cameron, L., Demeyere, B., Henckaerts, JB., La Haye, E., Niebergall-Lackner, H. (2015). The updated Commentary on the First Geneva Convention – a new tool for generating respect for international humanitarian law. *International Review of the Red Cross,* Vol. 97 (900), 1209-1226.

12. Carl Haas, M., Fischer, SC. (2017). Evolution of targeted killing practices: autonomous weapons, future conflict and international order. *Contemporary Security Policy*, Vol. 38(2), 281-306.

13. Clarke, R. (1993). Asimov's laws of Robotics: implications for information technology. *Computer*, Vol. 26(12), 53-61.

14. Crootof, R. (2018). Autonomous Weapon Systems and the Limits of Analogy. *Harvard National Security Journal*, Vol 51, 51-83.

15. Debuf, E. (2015). Tools to do the Job: The ICRC's legal status, privileges and immunities. *International Review of the Red Cross*, Vol 97(897-898), 319-344.
16. Dormann, K., Serralvo, J. (2014). Common Article 1 to the Geneva Convention and the obligation to prevent international humanitarian law violations. *International Review of the Red Cross*, Vol.96(895-896), 707-736.

17. Egeland, K. (2016). Lethal Autonomous Weapon Systems Under International Humanitarian Law. *Journal of International Law* Vol. 85 (2), 89-118.

18. Fleischman, F. (2015). Just say "no!" to lethal autonomous robotic weapons. *Journal of Information, Communication and Ethics in Society*. Vol 13(3/4), 299-313.

19. Grut, C. (2013). The Challenge of Autonomous Lethal Robotics to International Humanitarian Law. *Journal of Conflict & Security Law*, Vol 18(1), 5-23.

20. Haas, M., Fischer, S-C. 'Evolution of targeted killing practices: autonomous weapons, future conflict and international order' (2017) Contemporary Security Policy 38, 281-306.

21. Haataja, S. (2017). 2007 Cyber Attacks against Estonia and international law on the use of force: an informational approach, *Law, Innovation and Technology*, 9:2, 159-189.

22. Herve, A. (2016). Article 31 of the Vienna Convention on the Law of Treaties and Investment Law. *ICSID Review- Foreign Investment Law Journal*, Vol. 31(2), 366-387.

23. Hevelke, A., Nida-Rumelin, J. (2015). Responsibility for Crashes of Autonomous Vehicles: An Ethical Analysis. *Science & Engineering Ethics*, Vol.21(3), 619-630.

24. Horvitz, A., Nehs, R. (2011). Proportionality and international humanitarian law: an economic analysis. *Global Change, Peace & Security*, Vol. 23(2), 195-206.

25. Klincewicz, M. (2015). Autonomous Weapons Systems: the Frame Problem and Computer Security, *Journal of Military Ethics,* Vol. (14)(2), 162-176.

26. Kriner, D., Shen, F. (2014). Responding to War on Capitol Hill: Battlefield Casualties, Congressional Response, and Public Support for the War in Iraq. *American Journal of Political Science,* Vol.58 (1), 157-174.

27. Linderfalk, U. (2007). Is the Hierarchical Structure Of Article 31 and 32 of the Vienna Convention Real or Not? Interpreting the Rules of Interpretation. *Netherlands International Law Review*, Vol. 54(1), 133-154.

28. McDonald, N. (2019). The Role of Due Diligence In International Law. *International & Comparative Law Quarterly*, Vol 68 (4), 1041-1045.

29. Mcgrogan, D. (2014), On the Interpretation of Human Rights Treaties and Subsequent Practice. *Netherlands Quarterly of Human Rights*, Vol. 32(4), 347-378.

30. Roff, H. (2014). The Strategic Robot Problem: Lethal Autonomous Weapons in War, *Journal of Military Ethics*, Vol. 13(3), 211-227.

31. Van Den Boogaard, J. (2015). Proportionality and Autonomous Weapons Systems. *Journal of International Humanitarian Legal Studies*, Vol 6, 247-283.
32. van Kralingen, M. (2016). Use of Weapons: Should We Ban the Development of Autonomous Weapons Systems?. *The International Journal of Intelligence, Security and Public Affairs*, Vol 18:2, 132-156.

33. Rappert, B., Moyes, R., Crowe, A., Nash, T. (2012), The roles of civil society in the development of standards around new weapons and other technologies of warfare. *International Review of the Red Cross*, Vol. 94 (886), 765-785.

34. Schulzke, M. 'Autonomous Weapons and Distributed Responsibility' (2013) Philosophy & Technology 26, 203-219.

35. Sharkey, A.J. (2018). Autonomous weapons systems, killer robots and human dignity. *Ethics and Information Technology*, Vol. 21, 75-87.

36. Tsybulenko, E.; Platonova, A. (2019). Violations of Freedom of Expression and Freedom of Religion by the Russian Federation as the Occupying Power in Crimea. *Baltic Journal of European Studies*, Vol 9 (3 (28)), 134-147.

37. Wells-Greco, M. (2010). Operation 'Cast Lead': *Jus in Bello* Proportionality, *Netherlands International Law Review*, Vol. 57 (03), 397-422.

38. Zych, T. (2009). The Scope of the Obligation to Respect and to Ensure Respect for International Humanitarian law. *Windsor Yearbook of Access to Justice, Vol.* 27, 251-270.

EU and international legislation

39. Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field. Geneva, 27 July 1929.

40. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention), 12 August 1949, 75 UNTS 31.

41. International Convention against the Recruitment, Use, Financing and Training of Mercenaries, 4 December 1989.

42. 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.

43. Vienna Convention on the Law of Treaties (1969).

Other Sources

44. Boutruche, T., Sassoli M, 'Expert Opinion on Third States' Obligation vis-à-vis IHL Violations under International Law, with a special focus on Common Article 1 to the 1949 Geneva Conventions' < https://www.nrc.no/resources/legal-opinions/third-states-obligations-vis-a-vis-ihl-violations-under-international-law/> accessed 21 February 2020.

45. Jevglevskaja, N. (2018). Weapons Review Obligation under Customary International Law. *U.S. Naval War College International Law Studies,*Vol 94, 1-37.

46. McCormack, J. (1993). *One Million Mercenaries: Swiss Soldiers in the Armies of the World.* Barnsley, United Kingdom: Pen and Sword Books.

47. McGrath, J. (2007). The Other End of the Spear: The Tooth-to-Tail Ratio (T3R) in Modern Military Operations. *Combat Studies Institute Press*.

48. Schmitt, M., (2013). Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics. *Harvard National Security Journal Features*, 1-37.

49. Rivest, R. (1998). Case against regulating encryption technology. *Scientific American*, 116-117.

50. International Review of the Red Cross, Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 1st edition, (1952).

51. International Review of the Red Cross, Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 2nd edition, (2016).

52. International Review of the Red Cross, *Commentary on the Additional Protocols*, (1987).

53. ICRC, 'Practice Relating to Rule 10. Civilian Objects' Loss of Protection from Attack' <https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule10> accessed 23 December 2019.

54. ICRC, 'Practice Relating to Rule 14. Proportionality in Attack' <https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule14> accessed 23 December 2019.

55. Seaforces, 'Goalkeeper close-in weapon systems' <http://www.seaforces.org/wpnsys/SURFACE/Goalkeeper-CIWS.htm> accessed 23 December 2019.

Appendices

Appendix 1. Non-exclusive licence

Non-exclusive licence for reproduction and for granting public access to the graduation thesis[1]

I Aleksi Kajander (author's name)

1.Give Tallinn University of Technology a permission (non-exclusive licence) to use free of charge my creation

Making the Cyber Mercenary – Autonomous Weapons Systems and Common Article 1 of the Geneva Conventions ,
(title of the graduation thesis)

supervised by Agnes Kasper and Evhen Tsybulenko,
(supervisor's name)

1.1. to reproduce with the purpose of keeping and publishing electronically, including for the purpose of supplementing the digital collection of TalTech library until the copyright expires;

1.2. to make available to the public through the web environment of Tallinn University of Technology, including through the digital collection of TalTech library until the copyright expires.

2. I am aware that the author also retains the rights provided in Section 1.

3. I confirm that by granting the non-exclusive licence no infringement is committed to the third persons' intellectual property rights or to the rights arising from the personal data protection act and other legislation.

---

[1] *The non-exclusive licence is not valid during the access restriction period with the exception of the right of the university to reproduce the graduation thesis only for the purposes of preservation.*