INDIVIDUAL CRIMINAL RESPONSIBILITY FOR WAR CRIMES RESULTING FROM THE USE OF AUTONOMOUS WEAPONS SYSTEMS

Ludmila Halajová*

Abstract: *Autonomous weapons systems (AWS) are one of the emerging modern military technologies that are attracting more and more attention of the international community. While they raise a lot of questions with respect to various fields of law, the biggest worry is that there will be no accountability for their wrongful use. This article focuses on the individual criminal responsibility for war crimes committed with the use of AWS. Four modes of responsibility, which could be potentially applied to AWS-related war crimes, are considered in turn with the aim of ascertaining, whether the current rules of international criminal law provide sufficient basis to assign responsibility for these crimes.*

Keywords: *autonomous weapons systems, AWS, individual criminal responsibility, war crime, direct and indirect perpetration, command responsibility, joint criminal enterprise*

I. INTRODUCTION

The response of international law to autonomous weapons systems (AWS), i.e. "weapons systems that, once activated, can select and engage targets without further intervention by a human operator",[1] is one of the biggest recent challenges brought by the rapid evolution of military technology. One of the major concerns with respect to the development and deployment of increasingly autonomous weapons is that they will create an "accountability gap". Given their autonomous capabilities, AWS might isolate humans from any culpability as it will be unjust to hold any operators, developers, programmers, commanders and political leaders accountable for the acts of AWS, which would be beyond their sphere of influence. Accountability is an extremely important element of every legal system that functions as a deterrent of future violations. Without functional system of accountability for violations of the rules of international humanitarian law (IHL) resulting from the use of AWS, the maintenance of peace and security could be threatened alongside the victims' right to remedy.

Weapons were always just tools in the hands of soldiers and their impacts were easily traceable to particular persons using them. With the development of AWS the international community is faced with a potential weapon that could, to a large extent, act independently of any human oversight and therefore move from a simple tool to something more. Do AWS really introduce such a new variable into the equation that they create an accountability gap? Is there a need to develop new rules of international law that will help to assign responsibility for violations of international law using AWS? Or can AWS be

* Mgr. Ludmila Halajová is a Ph.D. candidate at the Faculty of Law, Charles University, Prague, Czech Republic

[1] DEPARTMENT OF DEFENCE. Directive No. 3000.09. Autonomy in Weapons Systems. In: *Executive Service Directorate* [online]. 21. 11. 2012 [2020-03-23]. Available at: <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf>. pp. 13–14.

accommodated within the existing modes of responsibility? Moreover, a multitude of different individuals at various levels will be involved in the development and deployment of AWS, including programmers, manufacturers, operators or commanders. Can we track responsibility for a war crime resulting from the misapplication of IHL principles by AWS back to a programming error and to individual programmers? Will human operators and commanders maintain control over AWS sufficient enough for them to be found responsible for the actions of AWS? Is there any superior-subordinate relationship between the commander and the AWS for command responsibility to be applicable? Those are just some of the questions one can ask in relation to AWS and accountability.

AWS bring challenges with respect to all systems of accountability, including state responsibility or corporate liability. However, this article focuses exclusively on the attribution of individual criminal responsibility for potential war crimes committed using AWS, which will arguably be one of the key determinants in finding the technology legal or illegal under international law.

II. INDIVIDUAL CRIMINAL RESPONSIBILITY FOR WAR CRIMES

The vast majority of potential international crimes resulting from the use of AWS will fall into the category of war crimes, i.e. the serious violations of customary or treaty rules of IHL. Given the characteristics of AWS as advanced weapons systems, it is safe to assume that, once developed, they will predominantly be used in the context of armed violence, i.e. in international or non-international armed conflicts.[2] It is, under some circumstances, possible to imagine an AWS involved also in a crime against humanity or genocide,[3] but the focus of this article will be on war crimes only.

The International Criminal Tribunal for the former Yugoslavia (ICTY) set out the general definition of war crimes in *Tadič*, where it specified the conditions for a war crime to fall under the tribunal's jurisdiction. For an offence to be considered a war crime, the following conditions must be met: (a) the violation must constitute a serious infringement of a rule

[2] There is of course the possibility of AWS being used in the context of violence not reaching the threshold of armed conflict. Classification of a certain ongoing violent situation as an armed conflict or a mere internal disturbance already proved a very difficult task in the past (particularly in case of deployment of armed drones by the US in Pakistan, Yemen or Somalia). However, the first and foremost ambit of international law, that should be considered in relation AWS, is the law of armed conflict, and as such will be the focus of this article. The debate at the relevant international fora supports the presumption, that the primary regime governing the use of AWS will be IHL and that States generally intend to use AWS only in the context of armed conflict. See e.g. Report of the 2019 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems. In: *United Nations Documents* [online]. 25. 9. 2019 [2020-03-23]. Available at: <https://undocs.org/en/CCW/GGE.1/2019/3>; Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons. In: *International Committee of the Red Cross* [online]. 16. 3. 2016 [2020-03-23]. Available at: <https://shop.icrc.org/autonomous-weapon-systems.html?_store=default&_ga=2.243318085.1759594343.1573300497-669971834.1573300497>. pp. 7–22.

[3] AWS could in theory be used for example in the systematic attack on one's own civilian population to commit large-scale killings or in the attack on a selected group. It is, however, quite difficult to imagine a State so flagrantly "hunting" a particular group of its own civilians selected by the AWS for example on the basis of their ethnicity.

of IHL, which protects important values and the breach of which involves grave consequences for the victims, (b) the rule must be customary in nature or follow from an applicable treaty and (c) the violation of that rule must entail the individual criminal responsibility of the person breaching the rule.[4]

Similar to other international crimes (and crimes in general), war crimes consist of both objective and subjective elements. The objective structure of a war crime encompasses conduct, consequences and causal nexus. Since no universal and legally binding list of all war crimes exists in international law, the objective elements of war crimes must be inferred from the substantive rules of IHL.[5] The Geneva Conventions and their Additional Protocol I. contain war crimes among their provisions relating to the so-called grave breaches.[6] Article 8 of the Rome Statute of the International Criminal Court (ICC)[7] contains the current most exhaustive list of war crimes and the statutes of ICTY[8] and International Criminal Tribunal for Rwanda (ICTR)[9] enumerate war crimes as well. Quite a lot of war crimes could be perpetrated using AWS, most notably crimes committed using prohibited means or methods of warfare. The crimes that involve intentionally directing an AWS against prohibited targets or launching of an AWS equipped with a banned weapon are not the primary source of worry among international lawyers in relation to AWS. The probability of such crimes occurring is very low and, in any case, the individual criminal responsibility in such cases should be relatively easy to establish. On the other hand, in cases where the AWS independently performs wrong assessment of the principles of distinction or proportionality the individual criminal responsibility would be much harder to establish and trace back to a specific individual.

The criminal responsibility for war crimes arises when the perpetrator possesses *mens rea*, a particular state of mind required for the offence. The required *mens rea* is sometimes specified by the relevant rule prohibiting certain conduct, but certainly not in every case. Most war crimes require the intent (*dolus directus*), as "an awareness that by engaging in a certain action or by omitting to act one shall bring about certain result and

[4] *Prosecutor v Tadič* (Interlocutory Appeal on Jurisdiction). ICTY-94-1 (2 October 1995), para. 94.

[5] CASSESSE, A. (ed.). *Cassese's International Criminal Law*. 3rd ed. Oxford: Oxford University Press, 2013, p. 70.

[6] Geneva Convention for the amelioration of the condition of the wounded and sick in armed forces in the field (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 31 (Geneva I.) art 50; Geneva Convention for the amelioration of the condition of the wounded, sick and shipwrecked members of the armed forces at sea (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 85 (Geneva II.) art 51; Geneva Convention relative to the treatment of prisoners of war (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135 (Geneva III.) art 130; Geneva Convention Relative to the Protection of Civilian Persons in Time of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 287 (Geneva IV.) art 147; Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (adopted 08 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Protocol I.) Art 85.

[7] Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) 2187 UNTS 3 (Rome Statute), art. 8.

[8] UNSC. Statute of the International Criminal Tribunal for the Former Yugoslavia. In: *ICTY* [online]. 25. 5. 1993 [2019-07-12]. Available at: <http://www.icty.org/x/file/Legal%20Library/Statute/statute_sept09_en.pdf>. Art. 2–3.

[9] UNSC. Statute of the International Criminal Tribunal for Rwanda. In: *United Nations International Residual Mechanism for Criminal Tribunals* [online]. 8. 11. 1994 [2020-03-23]. Available at: <http://unictr.irmct.org/sites/unictr.org/files/legal-library/100131_Statute_en_fr_0.pdf>. Art. 4.

the will to cause such result"[10]. There is no doubt that when the substantive rules of international criminal law (ICL) use the word "wilful", the perpetrator will be held criminally liable only if he acted with intent. Individual criminal responsibility will therefore be contingent upon intent for example in case of wilful killing or wilfully causing great suffering or serious injury to body or health according to the Geneva conventions.[11] Article 85 of the Additional Protocol I. also criminalizes grave breaches "when committed wilfully, in violation of the relevant provisions of [the] Protocol, and causing death or serious injury to body or health".[12] Sometimes the rules require "knowledge", which can either be part of intent as an awareness of the circumstances forming part of the crime's definition or denote recklessness (indirect intent or *dolus eventualis*).[13] In the case of recklessness the perpetrator is aware (knows) of the risk, that a certain conduct may violate some rule of IHL (e.g. the use of a weapon may entail killing a large number of civilians), but willingly takes the risk. The perpetrator does not necessarily desire the adverse consequences of his conduct but only envisages the result as possible or likely and deliberately takes the risk.[14] When international rules do not provide (explicitly or implicitly) for a subjective element, it could be inferred from the subjective element required for the underlying offence (e.g. murder, torture, rape, destruction of private property).[15] This, however, will not usually be the case of war crimes committed with the use of AWS. The majority of such crimes will not have this double-layered structure (i.e. will not be formed by underlying offence similar to one found in domestic legal systems accompanied by the international element), but will follow directly from the rules of IHL. When the subjective element of a crime cannot be found amongst the rules of IHL, the statutes of ICC and ICTY or ICTR can be of some help. Nevertheless, the statutes primarily set out conditions for their jurisdiction and not universal substantive rules of ICL. Any universal rules for *mens rea* therefore have to be picked up from the whole body of ICL including customary law.

International law does not generally require the perpetrator to possess a certain status in order for him to be found responsible for a war crime. War crimes may be perpetrated by combatants as well as civilians by one party to the armed conflict against persons or property of the other party.[16] In recent years, some military functions have frequently been "outsourced" and performed by non-military personnel.[17] Even though it is presumed that the deployment of AWS will be under the control of the military in the first place,[18] civilian personnel may get involved in some operations as well. While there might be some diffi-

[10] CASSESSE, A. (ed.). *Cassese's International Criminal Law*. 2013, p. 43.
[11] Geneva I., art. 50; Geneva II., art. 51; Geneva III., art. 130; Geneva IV., art. 147.
[12] Although according to the commentary, the term "wilful" in this article covers both intent and recklessness. See: PILLOUD, C. (et. al.). *Commentary on the additional protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. Geneva: Martinus Nijhoff Publishers, 1987. para 3474.
[13] CASSESSE, A. (ed.). *Cassese's International Criminal Law*. 2013, p. 76.
[14] Ibid., pp. 41, 45–49.
[15] Ibid., p. 76.
[16] Ibid., p. 67; GILL, T. D., FLECK, D. (ed.). *The Handbook of the International Law of Military Operations*. 2nd ed. Oxford: Oxford University Press, 2017, p. 548.
[17] Consider e.g. the use of armed drones by the CIA, the US national intelligence agency.
[18] See infra notes 52, 69.

culties with classifying civilian personnel operating or supervising AWS as combatants or persons directly participating in hostilities, their status is irrelevant as far as the individual criminal responsibility for war crimes is concerned since, in principle, anybody can commit a war crime as long as it is perpetrated during an armed conflict.[19] Not all crimes committed during an armed conflict constitute war crimes. In order for a crime to be qualified as a war crime it must be closely related to the armed conflict.[20] Crimes committed using AWS in the course of armed conflict will undoubtedly be closely related to that conflict and will pursue the aims of that conflict or contribute in some way to the overall military campaign. This is reinforced by the fact that the majority of envisaged crimes committed using AWS will fall into the category of violations of the rules on the conduct of hostilities and therefore the "war nexus" will be established easily. However, the war nexus requirement may preclude the attribution of responsibility to certain individuals (e.g. developers, manufacturers or programmers).

III. MODES OF CRIMINAL RESPONSIBILITY POTENTIALLY APPLICABLE

In this article I will not attempt to provide an exhaustive review of all modes of criminal responsibility assessing their applicability to the use of AWS. Instead, I will focus on those that are listed most often as potential basis for the attribution of responsibility in this context. Apart from direct perpetration I will consider indirect perpetration, superior or command responsibility and joint criminal enterprise. Sometimes the idea of AWS themselves being held responsible for the violations of international law comes into the question and it will be addressed briefly as well.

(A) Direct perpetration

In most situations the individual criminal responsibility follows when a person directly acts (or fails to act) in such a way, that his action (or omission) produces adverse consequences. In other words, the offender himself physically and personally perpetrates a crime or brings about culpable omission of an act required by a rule of ICL.[21] This mode of responsibility could come into play in relation to AWS only in the most straightforward violations, because in other instances the AWS itself would be the entity physically perpetrating the criminal act. Such straightforward violations can be found among the rules governing the methods as well as means of warfare and with respect to all of them direct intent is required to assign responsibility.

Regarding the use of prohibited means of warfare, individual criminal responsibility could arise from intentionally deploying AWS equipped with a prohibited weapon. Without any specific AWS in mind and without knowing what its construction and technical capabilities will be, we can assume that AWS as a weapons platform could be equipped with essentially any weapon imaginable. A weapon specifically prohibited under the treaty

[19] ZEMANEK, K. War Crimes in Modern Warfare. *Swiss. Rev. Int'l & Eur. L.* 2014, Vol. 24, pp. 215–217.
[20] CASSESSE, A. (ed.). *Cassese's International Criminal Law.* p. 77.
[21] *Prosecutor v Tadič* (Appeals Judgement). ICTY-94-1 (15 July 1999), para. 188.

or customary law could be integrated into AWS, e.g. biological[22] or chemical[23] weapon or a weapon prohibited under the Convention on prohibitions or restrictions on the use of certain conventional weapons[24] and its protocols. Moreover, any weapon integrated into AWS which causes superfluous injury or unnecessary suffering or which is inherently indiscriminate also violates international law.[25] A person, who intentionally deploys AWS with these types of weapons, either prohibited under treaty or customary law, is undoubtedly committing a war crime.[26] This type of violation would cause the least controversy regarding the attribution of responsibility since it would be quite easy to trace the responsibility for the deployment of such weapon back to the specific individual, who decided to integrate the prohibited weapon into the AWS. This would most likely be some commanding officer, who authorized or ordered such integration. With respect to this type of violation the autonomous features of the weapons platform are of no consequence and do not impede the attribution of responsibility.

With respect to prohibited methods of warfare, IHL for example prohibits making civilians the object of an attack.[27] If, in violation of this prohibition, civilians are wilfully targeted and this results in their death or serious injury, such act is considered a grave breach of Additional Protocol I.[28] and clearly a war crime.[29] However, if an AWS kills a civilian, did the human operator, who had activated its system, directly perpetrate the crime? The answer would probably depend on the degree of autonomy with which the AWS makes targeting decisions. If the operator issued some kind of order to the AWS to attack civilians or had the opportunity to influence the decision of the AWS in some way, the causal link between the operator's actions and the death of civilians would be established and he could be found guilty of a war crime.[30] Of course, there is then a question whether we can truly consider such system autonomous. Moreover, this type of war crime clearly requires direct intent on the part of the perpetrator. The individual criminal responsibility for the death of a civilian therefore cannot be tied to a mere activation of the AWS by a human operator. Direct intent requires that the perpetrator is aware of the victim's protected status. If the AWS is sufficiently autonomous in the targeting, the person who activates it will not be aware of any specific victims in advance and consequently will lack the necessary

[22] Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (adopted 10 April 1972, entered into force 26 March 1975) 1015 UNTS 163.

[23] Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction (adopted 3 September 1992, entered into force 29 April 1997) 1974 UNTS 45.

[24] Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (adopted 10 October 1980, entered into force 2 December 1983) 1342 UNTS 137.

[25] Protocol I., art. 35 (2), art. 51 (4); HENCKAERTS, J.-M., DOSWALD-BECK, L. *Customary international humanitarian law, Volume 1:Rules*. Cambridge: Cambridge University Press, 2005. Rule 70-71, pp. 237–250.

[26] Rome Statute, art. 8(2)(b)(xvii)-(xx), art. 8(2)(e)(xiii)-(xv); ICTY Statute, op. cit. sub 8, art. 3(a).

[27] Protocol I., art. 48, art. 51(2); Customary IHL, op. cit. sub 25, Rule 1, pp. 3–8.

[28] Protocol I., art. 81(3)(a).

[29] Protocol I., art. 81(5); Rome Statute, art. 8(2)(b)(i), art. 8(2)(e)(i); ICTY Statute, op. cit. sub 8, art. 2(a); ICTR Statute, op. cit. sub 9, art. 4(a).

[30] ZEMANEK, K. *War Crimes in Modern Warfare*. pp. 221–222; MCDOUGALL, C. Autonomous Weapon Systems and Accountability: Putting the Cart before the Horse. *Melb. J. Int'l L.* 2019, Vol. 20, p. 69.

mens rea.[31] If we focus on the situation, when AWS independently decides to attack a civilian, i.e. when it selects and engages specific target independent of any external intervention, the mode of direct perpetration fails, as there is no human perpetrator available, who would have intended for AWS to attack civilians.

Another example, quite AWS-specific, would be developing or programming AWS in such a way that it would not be able to make proper analysis that is required to satisfy the relevant principles of IHL. Careful application of the obligation to conduct reviews of newly studied, developed, acquired or adopted weapons, means or methods of warfare assessing their legality under IHL, stipulated in Article 36 of the Additional Protocol I., should effectively preclude the integration of such AWS into the armed forces. However, for the purposes of this article, let us suppose that such faulty AWS would, for various reasons, be put to use.[32] There are two problems with establishing individual criminal responsibility for direct perpetration of any war crime under such scenario. The first is the requirement of direct intent. The developers or programmers would have to intentionally develop the specific AWS with knowledge, that it would not adhere to the rules of IHL and that it could cause severe harm or death to protected persons (or damage to protected objects) due to its inability to adequately distinguish between potential targets or calculate military advantage in relation to incidental harm. It is quite unimaginable that developers would go to such lengths that they would consciously spend overwhelming time and resources to develop a weapon, that would be unlawful per se. At most, developers could be negligent or reckless in the development of an AWS and consciously disregard or overlook its ill-performances during testing and deem it ready to use even with high risk of misbehaviour (e.g. due to budget constraints or political pressure to put new technology in use).[33] However, their *mens rea* in such situations would not satisfy the level required for direct perpetration. The second problem flows from the requirement of war nexus, i.e. for a war crime to be closely related to an armed conflict. The developing and programming of a weapon system usually takes place a long time, often years, before its deployment in an actual armed conflict is even considered. Would the programming of an AWS not to follow the relevant rules of IHL without any connection to a specific armed conflict

[31] FORD, C. M. Autonomous Weapons and International Law. *S. C. L. Rev*. 2017, Vol. 69, p. 467.

[32] It should be noted that international law does not provide detailed rules on the conduct of legal reviews of new weapons and States are allowed considerable discretion over how they implement the obligation. States are very reluctant to share information about their review processes. Consequently, there is little information available about the state practice to assess the extent to which States comply with the obligation. It may therefore be possible that States will conduct unsatisfactory review during the development of AWS. See e.g. RAPPERT, B., MOYES, R., CROWE, A., NASH, T. The roles of civil society in the development of standards around new weapons and other technologies of warfare. *International Review of the Red Cross*. 2012, Vol. 94, No. 886, pp. 781–782.

[33] Hopefully a very unlikely scenario, that is nevertheless frequently considered by academics as a theoretical possibility See e.g. KALMANOVITZ, P. Judgement, liability and risks of riskless warfare. In: N. Bhuta (ed.). *Autonomous weapons systems: Law, Ethics, Policy*. Cambridge: Cambridge University Press, 2016, pp. 159–160; SARTOR, Giovanni; OMICINI, A. The autonomy of technological systems and responsibilities for their use. In: N. Bhuta (ed.). *Autonomous weapons systems: Law, Ethics, Policy*. Cambridge: Cambridge University Press, 2016, p. 63, BACKSTROM, A., HENDERSON, I. 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*. 2012, Vol. 94, No. 886, pp. 507–509.

satisfy the war nexus requirement? For a criminal act to be closely related to an armed conflict, the conflict "must play a substantial role in the perpetrator's decision, in his or her ability to commit the crime or in the manner in which the conduct was ultimately committed".[34] On the other hand, the armed conflict does not have to be the ultimate reason for the criminal conduct and it is not necessary to show, that armed conflict was occurring at the exact time and place as the criminal conduct.[35] If a programmer wrongly re-programmed the AWS with knowledge it would be used during a specific conflict, the nexus might be satisfied (irrespective of the location of the programmer, which could arguably be far away from the battleground). Since the rules of ICL require that the criminal conduct took place in the context of and was associated with a specific armed conflict,[36] with respect to programming or developing of AWS, that occurs prior to any conflict, the war nexus would not be present.[37] The individual criminal responsibility of programmers or developers in this case cannot be stretched so far as to cover an unlimited number of potential violations, that their creation could cause.

In any case, the responsibility of developers and programmers under the direct perpetration mode would most likely be barred either by the lack of *mens rea*, or by the lack of war nexus. To commit a war crime, they would always need to act through or with the help of another person or entity (maybe with the exception of an unlikely case when a programmer inserts wrong code into an AWS during its deployment in an armed conflict with a specific criminal act in mind, acting de facto as the system's operator). The modes of criminal responsibility more likely applicable to developers and programmers in certain situations would be the indirect perpetration, participation in join criminal enterprise or aiding and abetting (provided there is a principal perpetrator found culpable). The absence of a war nexus and the question of establishing required *mens rea* would however still be major challenges.

(B) Indirect perpetration

Given the abovementioned difficulties with finding the direct human perpetrator, some suggest indirect perpetration as a possible way of assigning individual criminal responsibility for war crimes committed by AWS. Under this mode, the indirect perpetrator uses another to physically commit the crime. Indirect perpetration is specifically enumerated in the Article 25(3)(a) of the Rome Statute, which states that a person shall be criminally responsible for a crime within the Court's jurisdiction if he commits such crime "through another person, regardless of whether that other person is criminally responsible".Although the Article 7 of the ICTY Statute and the Article 6 of the

[34] *Prosecutor v Lubanga* (Decision on the Confirmation of the Charges). ICC-01/04-01/06-803 (29 January 2007), para. 287; *Prosecutor v Katanga* (Decision on the confirmation of charges). ICC-01/04-01/07 (30 September 2008), para. 380.

[35] *Prosecutor v Tadič* (Trial Judgement and Opinion). ICTY-94-1 (7 May 1997), para. 573.

[36] INTERNATIONAL CRIMINAL COURT. Elements of Crimes. In: *International Criminal Court* [online]. 2013 [2020-03-23]. Available at: <https://www.icc-cpi.int/resource-library/Documents/ElementsOfCrimes Eng.pdf>. p. 9.

[37] MCFARLAND, T., MCCORMAC, T. Mind the Gap: Can Developers of Autonomous Weapons Systems Be Liable for War Crimes. *Int'l L. Stud. Ser. US Naval War Col.* 2014, Vol. 90, p. 374.

ICTR Statute do not expressly include indirect perpetration among the modes of individual criminal responsibility, both tribunals acknowledged and applied this mode in their rulings.[38] Indirect perpetration usually occurs in cases where the direct perpetrator is not fully criminally responsible for his actions (e.g. crimes committed using child soldiers). However, in certain situations both direct and indirect perpetrators can be found criminally responsible. The direct perpetrator could be responsible for his fulfilment of the subjective and objective elements of the crime and the indirect perpetrator for his control over the crime through his control over the direct perpetrator.[39]

The direct perpetrator, i.e. the person physically carrying out the deed, is often described as a "tool" or an "instrument" of a crime used by the indirect perpetrator. It is therefore not surprising that this mode of responsibility has a certain lure in relation to AWS.[40] Some authors argue that, for the purposes of assigning responsibility for war crimes committed using AWS, these should be treated as instruments used by the indirect perpetrator, who would most probably be a commanding officer of a high enough rank to oversee the relevant AWS deployment or possibly a programmer.[41] There is, of course, the problem that under the doctrine of indirect perpetration the "tool" has always been a person.[42] This begs a question whether the doctrine could cover a non-human entity as well. Given the culpability or non-culpability of a direct perpetrator is no longer decisive for the responsibility of an indirect perpetrator,[43] it is not entirely without reason to claim that the AWS as an executor of the crime could bear resemblance to the direct perpetrator. The nature of the "instrument" of indirect perpetration could be without consequence as long as it satisfies the relevant *actus reus* and is under the control of the indirect perpetrator. David Ohlin for example argues that the ability of AWS to exercise independent judgement does not exclude the responsibility of the indirect perpetrator. As long as the criminal action of the AWS is under the control of the indirect perpetrator, who sets its tasks, the system is allowed a considerable discretion over how it achieves them and military commanders could be held responsible for perpetrating war crimes through AWS.[44]

[38] CASSESSE, A. (ed.). *Cassese's International Criminal Law*. p. 179.

[39] *Prosecutor v Katanga* (2008), para. 497.

[40] It is a model considered not only by international lawyers, but by experts on criminal law as well. For some thoughts on ‚perpetration-by-another liability' as a model of criminal liability possibly applicable to autonomous vehicles under US criminal law see HALLEVY, G. Unmanned Vehicles: Subordination to Criminal Law under the Modern Concept of Criminal Liability. *Journal of Law, Information and Science*. 2011/2012, Vol. 21, No. 2, pp. 201–204.

[41] See e.g. OHLIN, J. D. The Combatant's Stance: Autonomous Weapons on the Battlefield. *Int'l L. Stud. Ser. US Naval War Col.* 2016, Vol. 92; MCDOUGALL, C. Autonomous Weapon Systems and Accountability: Putting the Cart before the Horse. *Melb. J. Int'l L.* 2019, Vol. 20, pp. 69–70; FORD, C. M. *Autonomous Weapons and International Law*. p. 467.

[42] Consider for example the wording of the Rome Statute, art. 25(3)(a).

[43] Rome Statute, art. 25(3)(a); *Prosecutor v Katanga* (2008), para. 495–496; *Prosecutor v Stakič* (Trial Judgement). ICTY-97-24 (31 July 2003), para. 741.

[44] OHLIN, J. D. *The Combatant's Stance: Autonomous Weapons on the Battlefield*. pp. 9–10, 21.

There might be another aspect of this mode of responsibility relevant to AWS. AWS will not be a solitary unit, but rather a part of an enormous multi-layered system. Apart from all the components creating the system's hardware and software there will be a multitude of people involved in the programming, developing, procuring and manufacturing of the system, as well as a number of operational commanders, analysts and other military personnel. Moreover, given the controversy around AWS, involvement of political leaders and governmental or parliamentary review bodies is expected.[45] All these components resemble a machine-like organization. Rather than seeing AWS as an individual entity that substitutes a single human perpetrator, we could possibly look at the situation in terms of collective and organizational criminality. Quite a number of works on AWS and responsibility rightly note that there will be so many individuals involved around AWS that it would be extremely hard or almost impossible to effectively distribute responsibility among them.[46] The international judicial bodies used the doctrine of indirect perpetration several times to address crimes committed through another by means of control over organization. It is possible to hold higher-level political and military leaders responsible as indirect perpetrators when they use an organized and hierarchical apparatus of power as an instrument of criminality.[47] ICL deals only with the most serious crimes that concern the international community as a whole and as such it is tasked with prosecuting high-level politicians and military officers, i.e. the top of the machinery. The ICC therefore argues that by specifically regulating the commission of a crime through another responsible person the Rome Statute targets organizational crimes.[48] In cases of large-scale crimes that involve hierarchical structure composed of many people on various levels engaged in various activities, the detachment of the political or military leader from the physical perpetration of the crime does not preclude his responsibility.[49] According to the ICC, the organized apparatus of power, that allows indirect perpetrator to commit crimes, must be based on strong hierarchical relationships between superiors and subordinates. The required authority and control over the organization exercised by the leader follows from the fact that his orders are generally complied with.[50] The control may take various forms (e.g. the capacity of the leader to hire, train, impose discipline and provide resources to his subordinates), but it should be such that the compliance with his orders is automatic and the subordinates are mere "cogs in the machine" that can be replaced quite easily.[51]

[45] BOOTHBY, W. H. Highly Automated and Autonomous Technologies. In: W. H. Boothby (ed.). *New Technologies and the Law in War and Peace*. Cambridge: Cambridge University Press, 2019, pp. 467–470.

[46] See e.g. MCFARLAND, T., MCCORMAC, T. *Mind the Gap: Can Developers of Autonomous Weapons Systems Be Liable for War Crimes*. p. 381; CHENGETA, T. Accountability Gap: Autonomous Weapon Systems and Modes of Responsibility in International Law. *Denv. J. Int'l L. & Pol'y*. 2016, Vol. 45, pp. 34–36.

[47] OHLIN, J. D. *The Combatant's Stance: Autonomous Weapons on the Battlefield*. pp. 8–14; *Prosecutor v Katanga* (2008), para. 495ff.

[48] *Prosecutor v Lubanga* (2007), para. 501.

[49] *Prosecutor v Katanga* (2008), para. 503.

[50] *Prosecutor v Katanga* (2008), para. 511–513.

[51] *Prosecutor v Katanga* (2008), para. 513, 515–518.

The military, which in most cases will be the organization deploying AWS,[52] arguably satisfies such requirements for hierarchical structure and compliance with the orders of the leadership. The leadership will order the deployment of an AWS in a particular operation and will set the basic framework for its operation (the geographical limits, time constraints, objectives, etc.). The difficulty arises with respect to the last requirement for the "organized apparatus of power" theory, i.e. the requirement that the leader uses his authority and power over the organization to execute crimes and that through his control over the organization the leader essentially decides whether and how the crime would be committed.[53]

With this last requirement, we return to the ever-present problem with the subjective element of the crime. Again, we can set aside the relatively uncontroversial cases when a commander intentionally uses military structures including AWS to commit specific war crimes, since in that case it should be quite easy to find him individually responsible. However, the occurrence of such cases is extremely unlikely. So how do we accommodate indirect perpetration into cases, where AWS violate the principles of distinction or proportionality in the course of their operation, when they have not been deployed by a military commander with a specific criminal act in mind? In that scenario, the commander will hardly have intended for an AWS to perform wrong assessment of a particular operational situation. If the commander could have reasonably believed that the AWS had ability to reliably perform the required analysis in the context of its deployment (given its capabilities, testing results, previous deployments etc.), then the situation is not that different from the use of conventional weapons and their failures. In that case the commander would be absolved of any responsibility for the adverse effects produced by AWS. If, on the other hand, the commander is aware of the facts suggesting, that the AWS will not be able to work properly in a certain operational reality and that there is a high risk of violating the relevant rules of IHL pertaining to the conduct of hostilities, and nevertheless orders the deployment of AWS, the situation is quite different. If the violation occurs, there is undeniably a connection between the commander's order to deploy AWS and the adverse consequences of that deployment.

[52] Based on the statements that States make at international fora and the fact, that they lay basis for the future use of AWS in their military manuals and directives, we can assume that they generally intend to integrate AWS into their military structures. See e.g. DEPARTMENT OF DEFENCE. Directive No. 3000.09. Autonomy in Weapons Systems. In: *Executive Service Directorate* [online]. 21. 11. 2012 [2020-03-23]. Available at: <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf>; EU statement at the 2019 meeting of the GGE on LAWS. In: *United Nations Geneva* [online]. 25. 3. 2019 [2020-03-23]. Available at: <https://www.unog.ch/80256EDD006B8954/(httpAssets)/7B83630931FB9850C12583CB003C96D4/$file/ALIGNED+LAWS+GGE+EU+statement+Military+Applications.pdf>; UK statement at the 2019 meeting of the GGE on LAWS. In: *United Nations Geneva* [online]. 25. 3. 2019 [2020-03-23]. Available at: <https://www.unog.ch/80256EDD006B8954/(httpAssets)/8B03D74F5E2F1521C12583D3003F0110/$file/20190318-5(c)_Mil_Statement.pdf>; Statement made by Germany at the 2019 meeting of the GGE on LAWS. In: *United Nations Geneva* [online]. 25. 3. 2019 [2020-03-23]. Available at: <https://www.unog.ch/80256EDD006B8954/(httpAssets)/95996F2E27AC3DE7C12583D2003D858F/$file/20190325+Statement1+Germany+GGE+LAWS.pdf>; and Israeli statement at the 2018 meeting of the GGE on LAWS. In: *United Nations Geneva* [online]. 9. 4. 2018 [2020-03-23]. Available at: <https://www.unog.ch/80256EDD006B8954/(httpAssets)/3F39A4A25049C9FCC1258272005789C6/$file/2018_LAWS6a_Israel.pdf>.

[53] *Prosecutor v Katanga* (2008), para. 514, 518.

The default *mens rea* requirement for war crimes is intent (*dolus directus*). The commander as indirect perpetrator has to know, that his actions or omissions relating to the deployment of AWS will lead to a commission of a specific war crime and he has to mean to cause such violation or be aware that his actions or omissions will bring about the commission of the war crime in the ordinary course of events.[54] This level of *mens rea* would never be satisfied by the commander who "only" ordered the deployment of AWS risking potential occurrence of non-specified violations of IHL. However, he could be found reckless in his deployment of AWS if he was aware of the strong possibility of the adverse outcome of his decision.[55] Recklessness, or *dolus eventualis*, covers situations where the perpetrator "is aware of the risk, that the objective elements of the crime may result from his actions or omissions, and accepts such an outcome by reconciling himself with it or consenting to it".[56] The ICC stated in the *Lubanga* case that if the perpetrator accepted, that the objective elements of a crime may result from his actions or omissions and reconciled himself with that possibility, such state of mind could be qualified as intent required under the Rome Statute.[57] Similarly, the ICTY in *Stakič* accepted *dolus eventualis* as sufficient to establish an intentional war crime of murder, if the perpetrator makes peace with the likelihood that his actions will cause death.[58] Although there is still some debate over whether only *dolus directus* is acceptable as a required mental state with respect to international crimes, there seems to be an agreement that unless a specific mental state is expressly required by the crime's definition, it is sufficient that the perpetrator is aware of the risk that the crime might be committed.[59]

Recklessness has evidently its place in ICL and it might serve well with respect to crimes physically committed by AWS under the control of a commander as indirect perpetrator. Although recklessness has not been addressed by international courts specifically in relation to indirect perpetration yet, it may nevertheless be a plausible way to hold high-ranking officers liable for at least some of the violations carried out by AWS. If the commander has a tight control over the military structures deploying AWS, he could be responsible for war crimes committed by AWS if he was aware of the strong likelihood of those crimes occurring and made peace with that likelihood. For example, the Commentary to the Additional Protocol I. states, that the war crime of wilfully launching an indiscriminate attack against the civilian population or civilian objects encompasses recklessness as "attitude of an agent who, without being certain of a particular result, accepts the possibility of it happening".[60] This conclusion, that the notion of wilfulness incorporates the concept of recklessness, was later accepted by ICTY in *Galič* case.[61]

---

[54] *Prosecutor v Lubanga* (2007), para. 350–352.
[55] OHLIN, J. D. *The Combatant's Stance: Autonomous Weapons on the Battlefield.* pp. 21–22.
[56] *Prosecutor v Lubanga* (2007), para. 352.
[57] *Prosecutor v Lubanga* (2007), para. 353–355.
[58] *Prosecutor v Stakič* (2003), para. 587.
[59] WERLE, G. Individual Criminal Responsibility in Article 25 ICC Statute. *J. Int'l Crim. Just.* 2007, Vol. 5, pp. 962–963.
[60] Commentary on the additional protocols (1987), op. cit. sub 12, para. 3474.
[61] *Prosecutor v Galič* (Trial Judgement). ICTY-98-29 (5 December 2003), para. 54–55.

There is, of course, a question whether it would be fair to convict a commander, who was "only" reckless in his deployment of the AWS, of the same war crime as a commander, who intentionally ordered targeting civilians. It is evident that the level of culpability differs in those situations and ICL is not equipped as well as national criminal systems to deal with culpability grading. Nevertheless, giving absolute leeway to the first commander does not seem right either. If the functionalities of a particular AWS were such that its operation in a particular scenario entailed high risk of bringing about for example the objective elements of a war crime of attacking civilians, the commander was aware of such risk and ordered the deployment anyway, such disregard for human life should warrant the attribution of responsibility to that commander.

(C) Superior (command) responsibility

A superior in an organized civilian or military unit has a special position within the system of ICL. In addition to the possibility of being found guilty of ordering a commission of a war crime,[62] he can be found responsible for the crimes of his subordinates on basis of his failure to supervise them adequately. The superior responsibility is covered by the statutes of both ICTY[63] and ICTR[64] as well as by the Rome Statute[65] and is considered a rule of customary international law.[66] In order to hold a superior responsible for the crimes of his subordinates, the following conditions must be met: a) the existence of a superior-subordinate relationship, b) knowledge of the involvement of the subordinates in a crime and c) superior's failure to prevent the commission of the crime or to punish subordinates.[67] Under the Rome Statute the additional element of causation is required, i.e. the commission of the crime by subordinates must occur as a result of superior's failure to exercise control.[68] The Rome Statute also sets a slightly different *mens rea* requirement for military and civilian superiors. Since AWS will most likely be used primarily within the military,[69] I will focus only on the responsibility of military commanders. The responsibility of political leaders can be established under this mode as well,[70] but given the difficulties discussed below, they would be too far removed from the violation to satisfy the requirements for the attribution of responsibility.

---

[62] Customary IHL, op. cit. sub 25, Rule 152, pp. 556–558.
[63] ICTY Statute, op. cit. sub 8, art. 7(3).
[64] ICTR Statute, op. cit. sub 9, art. 6(4).
[65] Rome Statute, art. 28.
[66] CASSESSE, A. (ed.). *Cassese's International Criminal Law*. p. 186; Customary IHL, op. cit. sub 25, Rule 153, pp. 558–560; *Prosecutor v Delalič and others* (Trial Judgement). ICTY-96-21 (16 November 1998), para. 333, 343.
[67] *Prosecutor v Delalič* (1998), para. 346.
[68] CASSESSE, A. (ed.). *Cassese's International Criminal Law*. p. 187.
[69] On military application see supra note 52. The effective development and use of such advanced technology requires considerable expertise, infrastructure and financial resources that at this point only States have access to. Therefore, States will be the first actors with the ability to effectively develop, manufacture and put to use AWS. The acquisition (e.g. via illicit market or by means of the „capture" of certain AWS and the copy of the software and hardware) and the use of AWS by non-state actors is a theoretical possibility that should be considered as well when debating the potential international regulation of AWS, but at first it is practical to focus on the role of States and military application.
[70] *Prosecutor v Delalič* (1998), para. 356.

Command responsibility usually comes first to the mind of those looking for a way to assign responsibility for war crimes committed while deploying AWS. It might be the most viable option for attributing responsibility to those overseeing the relevant deployment, but there is a number of obstacles with its application. While considering the command responsibility, I will focus exclusively on those types of violations, where the deployment of AWS is not inherently unlawful, but where during its deployment the AWS makes an autonomous operational decision, applying its artificial reasoning and machine learning capabilities, that results in a violation of the rules of IHL on the conduct of hostilities.[71]

First, the rules on command responsibility require that there exists a superior-subordinate relationship and that the commander exercises effective control over the acts of his subordinates, who commit international crimes. The mere formal status as a commander therefore does not suffice to establish responsibility. There is, therefore, a certain threshold beyond which the power of a superior to control his subordinates is too weak, remote or virtually non-existent to hold him justly responsible for the subordinates' crimes.[72] Superior only has effective control over his subordinates when he has the material ability to prevent or punish their criminal acts.[73] This first requirement raises two major questions with regard to the application of command responsibility in case of AWS: whether AWS can be considered subordinates and to what degree will commanders be able to control AWS.

The superior-subordinate relationship has always been understood as a relationship between human commanders and human soldiers and officers. To view relationship between AWS and its human operator or a mission commander as analogous to the superior-subordinate relationship is questionable at best.[74] To large extent, the basis for a functioning superior-subordinate relationship forms during military training and through the following of strict military discipline, which is something hardly transferable to the human-machine context.[75] On the other hand, the rules on command responsibility focus on the control rather than on the formal classification of the superior-subordinate relationship. The labelling of AWS as subordinate could therefore be irrelevant as long as the requirement of effective control of a commander over the AWS

[71] Despite a rigorous testing during development and established processes on human control and intervention during deployment, there will likely remain a discretionary space for an AWS to make choices other than those strictly envisioned by its programmers and operators. Such possibility is inherent in its autonomous character and the ability to learn from experience and surroundings. See e.g. SPARROW, R. Killer Robots. *Journal of Applied Philosophy*. 2007, Vol. 24, p. 70; BOOTHBY, W. H. *Highly Automated and Autonomous Technologies*. pp. 142–145.

[72] *Prosecutor v Delalič* (1998), para. 377.

[73] *Prosecutor v Delalič and others* (Appeals Judgement). ICTY-96-21 (20 February 2001), para. 256; Customary IHL, op. cit. sub 25, Rule 153, p. 561.

[74] See e.g. CHENGETA, T. *Accountability Gap: Autonomous Weapon Systems and Modes of Responsibility in International Law*. pp. 31–32; LIU, H-Y. Refining responsibility: differentiating two types of responsibility issues raised by autonomous weapons systems. In: N. Bhuta (ed.). *Autonomous weapons systems: Law, Ethics, Policy*. Cambridge: Cambridge University Press, 2016, pp. 332–333; CROOTOF, R. Autonomous Weapon Systems and the Limits of Analogy. *Harv. Nat'l Sec. J.* 2018, Vol. 9, pp. 68–73.

[75] For a different view see CORN, G. S. Autonomous weapons systems: managing the inevitability of 'taking the man out of the loop'. In: N. Bhuta (ed.). *Autonomous weapons systems: Law, Ethics, Policy*. Cambridge: Cambridge University Press, 2016. The author assimilates the development phase of AWS to the training of human soldiers and argues, that these phases are decisive for the compliance with the IHL rules.

is satisfied. However, the question of commander's ability to control AWS far exceeds the scope of this article. The extent to which humans will be able to retain control over AWS is one of the major issues continuously debated by academics and it is impossible to ascertain in advance without the knowledge of the particular system and the degree of its autonomy. The academics keep reminding that autonomy exists on a spectrum[76] and will vary amongst the different systems. The extent of commander's control over AWS will therefore be contingent upon the degree of AWS autonomy. In order for command responsibility to be applicable, the commander would have to retain such control over the actions of AWS to be able to materially influence its actions and override its decisions.[77]

As a second condition for command responsibility, the commander must know or have a reason to know that the crime is about to be committed or was committed. The commander must either have actual knowledge, that his subordinates were committing or about to commit crimes, or possess information, that would indicate the risk of crimes occurring.[78] Command responsibility is therefore not limited to cases, when commander has actual knowledge of the crimes, but applies also in instances of constructive knowledge, i.e. when the commander had information, which should have enabled him to conclude in the circumstances at the time, that his subordinates were committing or were going to commit a crime.[79] The information available to the commander does not have to be absolutely conclusive. It suffices that it indicates the need for additional investigation to ascertain whether the offences are about to be committed or were committed.[80] In case of constructive knowledge, the *mens rea* requirement will be satisfied also in cases of wilful blindness and conscious disregard with respect to criminal activities of the subordinates.[81] Compliance with this requirement in case of the use of AWS in theory does not differ significantly from its application with respect to conventional warfare. The commander will be expected to familiarize himself with the capabilities of weapons used in the military unit under his control. If he finds out, that a particular AWS cannot properly perform analysis required by the rules of IHL, such information would certainly be regarded as constructive knowledge in relation to crime committed later.[82] There will also arguably be mechanisms in place within the military to provide relevant information about the ongoing AWS deployment to the commanding structures. The problem with AWS with respect to information does not

[76] See e.g. MARRA, W. C., MCNEIL, S. Understanding the Loop: Regulating the Next Generation of War Machines. *Harv J L & Pub Pol'y*. 2013, Vol. 36, pp. 1155–60; SCHULLER, A. L. At the Crossroads of Control: The Intersection of Artificial Intelligence in Autonomous Weapon Systems with International Humanitarian Law. *Harv Nat'l Sec J*, 2017, Vol. 8, No. 2, p. 392; WAGNER, M. The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapon Systems. *Vand. J. Transnat'l L.* 2014, Vol. 47, p. 1379.

[77] Consider the concept of meaningful human control, e.g. in CHENGETA, T. Defining the Emerging Notion of Meaningful Human Control in Weapon Systems. *NYU J Int'l L & Pol.* 2017, Vol. 49, No. 3.

[78] *Prosecutor v Delalič* (1998), para. 383.

[79] Customary IHL, op. cit. sub 25, Rule 153, p. 562–563; Protocol I., art. 86(2).

[80] *Prosecutor v Delalič* (1998), para. 393.

[81] REITINGER, N. Algorithmic Choice and Superior Responsibility: Closing the Gap between Liability and Lethal Autonomy by Defining the Line between Actors and Tools. *Gonz. L. Rev.* 2015, Vol. 51, p. 108.

[82] FORD, C. M. Autonomous Weapons and International Law. *S. C. L. Rev.* 2017, Vol. 69, p. 474.

relate so much to their availability, but rather to the practical ability of a commander to act on them.[83]

Finally, command responsibility only applies if the commander fails to take the necessary and reasonable measures that are within his powers or at his disposal given the circumstances to prevent the criminal act or punish the perpetrator. What is necessary and reasonable will depend on the circumstances of the case, but the commander may generally be found responsible for not taking measures that are within his material ability.[84] In relation to AWS, the situation when a crime is about to be committed is more relevant. In such situation the commander can potentially intervene in the ongoing operation to prevent the violation and can be found responsible for his failure to do so. However, the timeframe for any override may be too narrow for a commander to intervene in any meaningful way. Improvements in technology already increase the tempo of the battle and the gradual distancing of humans from performing the critical functions follows that trend. Any oversight could be rendered meaningless if the timeframe for a commander to make an informed critical decision would be very small.[85] In a situation, when the crime already occurred, the doctrine of command responsibility would hardly be applicable under the current state of law, since it would be virtually impossible to punish a machine.[86] The commander would inevitably have to react to the wrongful action of AWS in some way, at least by conducting some kind of review of the problematic deployment or by checking the software and hardware settings of the system, but his failure to do so would hardly incur command responsibility for the violation in question. In *Blaškič* the Appeals Chamber of ICTY stated, that with respect to command responsibility the tribunal is "limited to showing that the accused had the power to prevent, punish, or initiate measures leading to proceedings against the alleged perpetrators where appropriate".[87] The requirement of "initiating measures leading to proceedings" could arguably translate to the use of AWS in the sense that the commander would not necessarily have to "punish" the AWS for the violation, but his failure to initiate a thorough review of the relevant deployment could incur his responsibility for the violation. Nonetheless, that stretches the doctrine too far in my view.

In any case, it is important to note that under the command responsibility the superior is not responsible for the crime of his subordinate but rather for his own omission to properly supervise him.[88] In other words, the commander will be responsible for his role in the occurrence of a war crime but not for the consequences of his subordinate's behaviour.[89]

---

[83] e.g. due to information overload and practical inability to sort quickly through the huge amount of information that is expected to be constantly flowing from the system's sensors.

[84] *Prosecutor v Delalič* (1998), para. 394–395; *Prosecutor v Blaškič* (Appeals Judgement). ICTY-95-14 (29 July 2004), para. 417.

[85] SPARROW, R. *Killer Robots.* p. 70; BOOTHBY, W. H. *Highly Automated and Autonomous Technologies.* p. 68; LIU, H-Y. *Refining responsibility: differentiating two types of responsibility issues raised by autonomous weapons systems.* pp. 333–334.

[86] The idea of AWS themselves being held responsible for war crimes is briefly addressed below.

[87] *Prosecutor v Blaškič* (2004), para. 69.

[88] FORD, C. M. *Autonomous Weapons and International Law.* p. 471.

[89] LIU, H-Y. *Refining responsibility: differentiating two types of responsibility issues raised by autonomous weapons systems.* pp. 338–340.

Therefore, even if the command responsibility could apply and the AWS could be perceived as superior's subordinate, responsibility gap in relation to the war crime committed by AWS itself would still remain.

(D) Joint criminal enterprise

As I have already mentioned, there will inevitably be many people on various levels involved in the development and use of AWS. The academics therefore naturally turn to a mode of responsibility that has been used in the past to deal with collective, systematic and widespread criminality in cases, where the exact level of every participant's contribution was hard to ascertain. The doctrine of joint criminal enterprise (JCE) was introduced in the *Tadič* Appeals Chamber judgement. The Chamber observed, that most of the crimes committed in wartime situation "do not result from the criminal propensity of single individuals but constitute manifestations of collective criminality: the crimes are often carried out by groups of individuals acting in pursuance of a common criminal design".[90] The concept of JCE acknowledges that even though only some members of a particular group may physically perpetrate the crime, the contribution of other members is usually vital in facilitating the commission of that crime. It is often extremely difficult to pinpoint the specific contribution made by each individual participant to the collective effort, but it would be unjust and against the purpose of the ICL if such behaviour would go unpunished.[91] For JCE to apply, multiple persons must be involved in the commission of a crime, they must share a common plan, design or purpose, which involves the commission of a crime, and the participant in JCE must in some way contribute to the execution of the common purpose.[92] It is, however, important to mention that JCE is a mode of individual criminal responsibility that evolved under the ICTY jurisprudence. The ICC has not yet embraced the concept and although the articles 25(3)(a) and 25(3)(d) of the Rome statute allow to impute responsibility to a person, who "commits a crime jointly with another" or who "in any other way contributes to the commission or attempted commission of such a crime by a group of persons acting with a common purpose", they establish respectively a form of co-perpetration and a residual form of accessorial liability rather than lay basis for the JCE.[93]

In *Tadič* the ICTY differentiated between three categories of collective criminality under the JCE. The first (and the most common) category includes cases where all perpetrators act pursuant to a common design and possess the same criminal intent.[94] The second category covers the so-called "concentration camp" cases. The doctrine of JCE was applied

[90] *Prosecutor v Tadič* (Appeals Judgement), para. 191.

[91] CASSESSE, A. The Proper Limits of Individual Responsibility under the Doctrine of Joint Criminal Enterprise. *J. Int'l Crimi. Just.* 2007, Vol. 5, p. 110.

[92] CASSESSE, A. (ed.). *Cassese's International Criminal Law.* p. 163; *Prosecutor v Tadič* (Appeals Judgement), para. 227.

[93] CASSESSE, A. (ed.). *Cassese's International Criminal Law.* p. 175; OLASOLO, H. Reflexiones Sobre la Doctrina de la Empresa Criminal Comun en Derecho Penal Internacional. *Inter-Am. & Eur. Hum. Rts. J.* 2009, Vol. 2, p. 159; SUMMERS, M. A. The Problem of Risk in International Criminal *Law. Wash. U. Global Stud. L. Rev.* 2014, Vol. 13, p. 670.

[94] *Prosecutor v Tadič* (Appeals Judgement), para. 196.

to situations of institutionalized criminal framework, where the offences were committed by members of units running concentration camps.[95] The third and most controversial category comprises situations, where one of the perpetrators deviates from the pursued aim and commits an act outside the common design that is nevertheless a natural and foreseeable consequence of furthering the common purpose.[96]

The first type of JCE would hardly cover war crimes committed with the use of AWS. Under that scenario the person involved would have to voluntarily participate in some aspect of the common design and even though he or she would not physically commit the violation (e.g. the killing of a civilian by AWS), such result would have to be his or her intent.[97] For JCE to apply, the person's involvement in the violation cannot be a random act. Rather, he or she needs to possess knowledge of the purpose of the criminal enterprise and share the intent with others. Although it is perhaps imaginable, that a group within the military could decide to use AWS to commit crimes, occurrence of such arrangement to commit violations of IHL is unlikely.

The second type of JCE is not very suitable to cover crimes committed with AWS either. Those crimes might fall under some form of organizational violence, but they would not resemble the concentration camp kind of scenario. To establish individual criminal responsibility in such cases there would have to be an organized system set up to commit various crimes, the accused would have to be aware of the true nature of the system and he would have to, in some way, actively participate in enforcing the system.[98] This type of JCE could possibly only apply if the military developed a framework, in which it would routinely use AWS to commit war crimes. Even though only some persons would be the ones physically perpetrating the crime,[99] the others could also bear the responsibility if they were aware of the crimes being perpetrated and willingly took part in the functioning of the military. There does not necessarily have to exist a previous plan or agreement, it suffices that each participant is cognizant of the crimes, in which the members of the military engage, and shares the intent to commit such crimes.[100] Under this scenario it would perhaps be possible to hold accountable the programmers and developers as well if they knew that they were contributing to an unlawful purpose. However, this legal construction would not serve well to cover the individual criminal responsibility in cases where the commanders, operators, programmers or manufacturers did not intend for AWS to commit war crimes, but those nevertheless occurred because the AWS in its autonomous functioning "chose" a course of action resulting in violations.

The third (and the most controversial) type of JCE is the one that could be potentially relevant to cases of AWS performing actions outside of the expected pre-programmed pa-

[95] Ibid., para. 202.
[96] Ibid., para. 204.
[97] Ibid., para. 196, 228.
[98] Ibid., para. 202, 220.
[99] E.g. equipping AWS with a prohibited weapon, deciding to employ AWS in a highly populated area when it is only capable of being used in unpopulated area or programming excessively high thresholds for collateral damage.
[100] The intent can be implicitly inferred from the fact, that the participant continues to participate in the criminal activity and does not abandon his function in the system. See CASSESSE, A. *The Proper Limits of Individual Responsibility under the Doctrine of Joint Criminal Enterprise*. pp. 112–113.

rameters. In that case, the responsibility arises if the participant did not have the intent to commit the incidental crime but was aware, that the actions of the group would most likely lead to its commission, and willingly took that risk (i.e. *dolus eventualis* suffices as *mens rea*).[101] This could translate to the use of AWS where the military personnel involved have not intended to use it to commit a war crime, but could have predicted its commission. The problem is that this mode supposes that the common plan shared by the participants is also of criminal nature. The perpetrators participate intentionally in a commission of one crime and, under certain circumstances, can be found responsible for other criminal acts incidental to the main one and committed only by some perpetrators.[102] According to the ICTY, the common plan "necessarily has to amount to, or involve, an understanding or an agreement between two or more persons that they will commit a crime within the Statute".[103] Regarding the subjective element, the ICTY clearly spelled out in *Tadič* that the participant must possess "the intention to participate in and further the criminal activity or the criminal purpose of a group and to contribute to the joint criminal enterprise or in any event to the commission of a crime by the group".[104] Then he can be found guilty of another crime, if it was a foreseeable consequence of furthering the initial common criminal purpose. The incidental crime should constitute a logical and predictable development of the original criminal plan shared by the perpetrators and it should be (at least abstractly) in line with the agreed criminal offence.[105] In other words, the incidental crime is an outgrowth of the previously agreed or planned criminal conduct for which each participant is already responsible.[106] It therefore follows that where military unit engages in lawful action and one member in the course of the operation commits a war crime, he alone should be held responsible and not all members of the unit under the doctrine of the JCE. The notion of JCE is always premised on sharing of a criminal intent by all those who take part in the enterprise.[107]

Would it be possible to refine and stretch the third type of JCE to cover cases when an AWS is used in the course of a lawful military operation (i.e. within lawful common purpose) but violates the rules of IHL for some reason? It could be a way to cover the situations where the aim of the operation and the use of AWS was in itself lawful, but there were indications known to commanders, operators, programmers or other involved persons that given the technical capabilities of the AWS and the characteristics of the operation the occurrence of violations was quite likely. The law should be able to respond to those situations and protect the international community from such reckless behaviour. However, under the current state of law the JCE would only be applicable if the design and use of

[101] SUMMERS, M. A. *The Problem of Risk in International Criminal Law.* p. 675.
[102] CASSESSE, A. *The Proper Limits of Individual Responsibility under the Doctrine of Joint Criminal Enterprise.* p. 113; *Prosecutor v Tadič* (Appeals Judgement), para. 206, 220; OLASOLO, H. *Reflexiones Sobre la Doctrina de la Empresa Criminal Comun en Derecho Penal Internacional.* pp. 160–161.
[103] *Prosecutor v Brdanin* (Trial Judgement). IT-99-36 (1 September 2004), para. 342.
[104] *Prosecutor v Tadič* (Appeals Judgement), para. 228.
[105] *Prosecutor v Tadič* (Appeals Judgement), para. 228; CASSESSE, A. *The Proper Limits of Individual Responsibility under the Doctrine of Joint Criminal Enterprise.* p. 113.
[106] CASSESSE, A. (ed.). *Cassese's International Criminal Law.* p. 118–119.
[107] Ibid., p. 126.

AWS was intended to perpetrate a certain war crime or to further a common criminal purpose of a group.[108] Then one could imagine that the persons involved (e.g. commanders, operators or programmers) could be found guilty of an incidental crime not initially envisaged under the common plan, if its occurrence was foreseeable given the AWS characteristics. In any case, even if it was accepted that the JCE could be used in cases where the primary common purpose of the group was lawful, there would still remain serious challenges in predicting the actions of AWS. It is not clear, under the current state of technological development, to what extent the actions of AWS would be predictable when operating under fully autonomous mode.[109] Moreover, similarly to the abovementioned modes of responsibility, the JCE functions on the premise that the deviating participant is a person and not a non-human entity. That could be an insurmountable obstacle in applying the doctrine to the context of AWS.

(E) Liability of AWS itself

Many authors briefly address the question whether AWS themselves could be held responsible for violations they cause. As autonomous entities they will be able to operate independently and make discretionary choices to engage specific targets without being programmed to do so in relation to individual cases. In theory, artificial intelligence could one day evolve to such an extent that machines will become very sophisticated and intelligent.

The fundamental argument against the notion of AWS being responsible themselves is the lack of moral agency in the machines, which is the key attribute of a human being that permits the ascription of responsibility.[110] For AWS to be responsible, they would have to be moral agents, i.e. they would need to possess an ability to make moral judgements based on some notion of right and wrong.[111] Even if machines could be found responsible, it would be nearly impossible to find a suitable form of punishment similar to those that are applied to human offenders. The only punishment theoretically equivalent to the incarceration is shutting down or destroying the system. But given the immense resources invested into the development and functioning of the system, states would certainly be unwilling to support such punishment. Moreover, shutting down the system would not

[108] FORD, C. M. *Autonomous Weapons and International Law.* p. 468.

[109] In order to be able to operate effectively in an armed conflict, AWS are expected to possess some kind of self-learning abilities, which would allow them to learn and adapt to such demanding and constantly changing environment in pursuit of open-ended tasks. Moreover, AWS software will likely be a very complicated combination of codes written by teams of programmers, where nobody will be able to predict and test all the ways in which the elements of the code may interact with each other. Unforeseen actions and errors of AWS may result not only from the unanticipated interactions between the parts of the same system but also from the contact with allies' and enemies' systems. See e.g. ZEMANEK, K. *War Crimes in Modern Warfare.* p. 223; CROOTOF, R. *Autonomous Weapon Systems and the Limits of Analogy.* pp. 59–62; KRUPIY, T. Unravelling Power Dynamics in Organizations: An Accountability Framework for Crimes Triggered by Lethal Autonomous Weapons Systems. *Loy. U. Chi. Int'l L. Rev.* 2017, Vol. 15, pp. 8–12.

[110] WAGNER, M. *The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapon Systems.* p. 1403; CHENGETA, T. *Accountability Gap: Autonomous Weapon Systems and Modes of Responsibility in International Law.* pp. 11–12.

[111] SPARROW, R. *Killer Robots.* pp. 71–73.

be very efficient since the code, on basis of which the AWS took the wrong decision, would likely be present amongst other systems.[112]

According to many authors, AWS will not take the form of sentient robots with a human-like artificial intelligence, at least not in any foreseeable future, given the immense difficulties with developing such technology.[113] When looking for ways to accommodate AWS within current system of individual criminal responsibility it is therefore not helpful to consider the possibility of AWS being themselves responsible for their actions. Since it is not currently possible to find AWS themselves responsible for war crimes, the accessorial mode of aiding and abetting fails too. Although it could theoretically capture the various contributions of human actors (i.e. operators, commanders, programmers or developers) to the war crime, it does not stand alone and is contingent upon finding the principal perpetrator culpable,[114] i.e. in this case the AWS itself.

IV. CONCLUSION

In ICL, as well as in national systems, the principle of personal culpability (or principle of individual criminal responsibility) represents one of the fundamental principles of criminal justice. According to this principle, nobody may be held criminally responsible for acts in which he has not personally engaged or in some other way participated.[115] There are fears, that with the development of AWS the individual criminal responsibility would either be unjustifiably stretched to cover persons that contributed to the crimes committed by AWS only very remotely or a system of organized irresponsibility for such crimes would emerge.

There are, as the previous sections of this article show, some modes of criminal responsibility in ICL that are theoretically capable of addressing, at least partially, the challenges posed by AWS. There are situations, where individual criminal responsibility for war crimes committed with the use of AWS could be assigned. However, the current framework of international law is incapable to respond to situations when the autonomous nature of AWS fully manifests (i.e. when the AWS makes a fully independent and unsupervised choice that results in a commission of a war crime) and when its conduct is unforeseeable and out of the effective control of any operator, commander, programmer or developer. Moreover, to apply almost all modes of criminal responsi-

[112] WAGNER, M. *The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapon Systems.* p. 1404.

[113] See e.g. REITINGER, N. *Algorithmic Choice and Superior Responsibility: Closing the Gap between Liability and Lethal Autonomy by Defining the Line between Actors and Tools.* pp. 91–92; HEYNS, C. Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions. UN Doc. A/HRC/23/47. para. 4. In: *Official Document System of the United Nations* [online]. [2020-03-23]. Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/127/76/PDF/G1312776.pdf?OpenElement>; SPARROW, R. *Killer Robots.* p. 70; p. 73; KALMANOVITZ, P. Judgement, liability and risks of riskless warfare. In: N. Bhuta (ed.). *Autonomous weapons systems: Law, Ethics, Policy.* Cambridge: Cambridge University Press, 2016, p. 155.

[114] MCDOUGALL, C. *Autonomous Weapon Systems and Accountability: Putting the Cart before the Horse.* pp. 78–79; CHENGETA, T. *Accountability Gap: Autonomous Weapon Systems and Modes of Responsibility in International Law.* p. 22; CASSESSE, A. *The Proper Limits of Individual Responsibility under the Doctrine of Joint Criminal Enterprise.* pp. 193–196.

[115] *Prosecutor v Tadič* (Appeals Judgement), para. 186.

bility discussed in this article, we would have to view AWS as analogous to humans at least in some aspect of the responsibility.[116] It is unclear whether the relevant rules of international law could be interpreted and applied in a way that accommodates a non-human entity.

One should also keep in mind that focusing on the individual commanders, operators, developers or manufacturers does not capture well the reality of the development and deployment of AWS. Behind each AWS there will be an enormous machinery of people at each stage of its life cycle. A sophisticated AWS will not be developed by a single individual, but rather by many teams of developers working on different components of the system.[117] The same is true for the subsequent deployment, in which many individuals, ranging from policy makers and military commanders to operators and analysts, will be involved. Attempting to identify individuals responsible for behaviour of a deployed AWS that constitutes a war crime may be too difficult for the purposes of initiating criminal proceedings. When working with such a complex system, there are two equally high risks: that of impunity on one hand and scapegoating on the other.[118] When the responsibility becomes diffused among too many actors, the link to the war crime might become so weak with respect to each individual that none will be found accountable and impunity will prevail. Conversely, if the existing rules on criminal responsibility are overly stretched to cover every contributor to the system, many people could end up being held accountable for something they had very little control over.

The only way forward under the current state of law seems to be the maintaining of a sufficient level of human control and oversight over the use of increasingly autonomous weapons and finding a common understanding on the elements of such control.[119] The exercise of certain control over weapon systems and the performance of autonomous functions are not mutually exclusive. Weapons will most likely never be either non-autonomous or fully autonomous. The degree of their autonomy will vary with time, mission phases or different tasks and functions. Even the most commonly used definition of AWS covers those that are human-supervised and "designed to allow human operators to override operation of the weapon system, but can select and engage targets without further

[116] E.g. an agent used by indirect perpetrator, a member of the JCE deviating from the common purpose or a commander's subordinate.

[117] MCFARLAND, T., MCCORMAC, T. *Mind the Gap: Can Developers of Autonomous Weapons Systems Be Liable for War Crimes*. p. 384; ZEMANEK, K. *War Crimes in Modern Warfare*. pp. 223.

[118] LIU, H-Y. *Refining responsibility: differentiating two types of responsibility issues raised by autonomous weapons systems*. pp. 326–327, 341.

[119] The Group of Governmental Experts of the High Contracting Parties to the Convention on Certain Conventional Weapons at its 2018 session agreed on guiding principles for further discussion at international level. One of the principles requires that "[h]uman responsibility for decisions on the use of weapons systems must be retained since accountability cannot be transferred to machines". Another principle adds, that "[a]ccountability for developing, deploying and using any emerging weapons system in the framework of the CCW must be ensured in accordance with applicable international law, including through the operation of such systems within a responsible chain of human command and control". See Report of the 2018 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems. CCW/GGE.1/2018/3. In: *United Nations Documents* [online]. 23. 10. 2018 [2020-03-23]. Available at: < https://undocs.org/en/CCW/GGE.1/2018/3>. Para 21.

human input after activation".[120] I do not believe that once the highly sophisticated and autonomous weapons systems are developed there will be no oversight whatsoever put in place within the militaries over their use. Some military personnel will always be tied to the deployment of AWS. Someone will have to set the mission parameters and objectives, program them into the system and monitor the mission. It is not only potentially unlawful to cease all control over a certain weapon system, but also impractical. It is arguably in the military's own interest to integrate AWS into its structures in such way that an effective and meaningful control over them is maintained.[121] More so, it is in the interest of those superiors, who will command the structures including AWS, not to risk the danger of being held responsible (whether under the international or domestic law) for something they had no effective means of controlling. Obviously, it will be extremely hard to find the ideal equilibrium between the human-machine collaboration. A right mix of the advantages of both "systems" will need to be found in order for the human control to remain effective but not to render any advantages of the system's autonomous features meaningless.

In any case, in order to avoid a system of organized irresponsibility, it will be necessary to determine who can be responsible for the use of AWS and under what circumstances prior to their fielding, i.e. preferably during the development stage. The proper measures to accommodate these systems within the processes of legal reviews of new weapons will need to be put in place to make sure they are developed in such a way that, despite their advanced autonomous capabilities, they will remain under the control of humans.

[120] DEPARTMENT OF DEFENCE. Directive No. 3000.09. Autonomy in Weapons Systems. In: *Executive Service Directorate* [online]. 21. 11. 2012 [2020-03-23]. Available at: <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf>. pp. 13–14.

[121] It is, however, helpful to consider whether responsibility for fully autonomous action of AWS could, in theory, be ever assigned to humans under the various modes of individual criminal responsibility, as has been attempted in this article. Some authors fear that although States now generally support the need to maintain sufficient human control over the critical functions of advanced weapons systems, there may be a pressure in the future to delegate that control to weapons system for tactical and operational reasons. See more in SPARROW, R. *Killer Robots.* pp. 68–69.