INTERNATIONAL LAW STUDIES

Published Since 1895

Autonomous Cyber Weapons and Command Responsibility

Russell Buchan and Nicholas Tsagourias

96 INT'L L. STUD. 645 (2020)

Volume 96

2020

Published by the Stockton Center for International Law

ISSN 2375-2831

Autonomous Cyber Weapons and Command Responsibility

Russell Buchan[*] *and Nicholas Tsagourias*[**]

CONTENTS

* Senior Lecturer in International Law, University of Sheffield. Author email: r.j.buchan@sheffield.ac.uk.

** Professor of International Law, University of Sheffield. Author email: nicholas.tsagourias@sheffield.ac.uk.

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

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

I. INTRODUCTION

Parties to armed conflicts frequently deploy cyber weapons and, recognizing the competitive advantages afforded by autonomy, States are developing—or perhaps have already developed—autonomous cyber weapons for use in armed conflict.[1] In this context, autonomy does not mean independence from humans because ultimately autonomous cyber weapons (ACWs) are programmed, deployed and can be supervised by humans.[2]

As a matter of fact, autonomy exists on a continuum[3] and the degree of autonomy possessed by a weapon is determined by its technical specification, the functions that have been automated, and the weapon's interaction with a human agent.[4] For example, cyber weapons have limited autonomy where

---

1. UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH, THE WEAPONIZATION OF INCREASINGLY AUTONOMOUS TECHNOLOGIES: AUTONOMOUS WEAPON SYSTEMS AND CYBER OPERATIONS (2017), https://unidir.org/files/publications/pdfs/autonomous-weapon-systems-and-cyber-operations-en-690.pdf; Dan Sabbagh, *Britain has Offensive Cyberwar Capability, Top General Admits*, GUARDIAN, Sept. 25, 2020, https://www.theguardian.com/technology/2020/sep/25/britain-has-offensive-cyberwar-capability-top-general-admits.

2. DEFENSE SCIENCE BOARD, U.S. DEPARTMENT OF DEFENSE, TASK FORCE REPORT: THE ROLE OF AUTONOMY IN DOD SYSTEMS 1–2 (2012), https://fas.org/irp/agency/dod/dsb/autonomy.pdf ("It should be made clear that all autonomous systems are supervised by human operators at some level, and autonomous systems' software embodies the designed limits on the actions and decisions delegated to the computer.").

3. *See* U.S. Department of Defense, DoD Directive 3000.09, Autonomy in Weapon Systems, (2012, incorporating Change 1, May 8, 2017), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf. Moreover, according to the U.K. Ministry of Defence,

> An autonomous system is capable of understanding higher-level intent and direction. From this understanding and its perception of its environment, such a system is able to take appropriate action to bring about a desired state. It is capable of deciding a course of action, from a number of alternatives, without depending on human oversight and control, although these may still be present. Although the overall activity of an autonomous unmanned aircraft will be predictable, individual actions may not be.

DEVELOPMENT, CONCEPTS AND DOCTRINE CENTRE, UNITED KINGDOM MINISTRY OF DEFENCE, JDP 0-30.2, UNMANNED AIRCRAFT SYSTEMS 13 (2017), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/673940/doctrine_uk_uas_jdp_0_30_2.pdf; *see also* DEVELOPMENT, CONCEPTS AND DOCTRINE CENTRE, UNITED KINGDOM MINISTRY OF DEFENCE, JCN 2/17, FUTURE OF COMMAND AND CONTROL (2017), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643245/concepts_uk_future_c2_jcn_2_17.pdf.

4. The human-machine interaction in the decision-making loop is schematically described as a "human in the loop," "human on the loop," and "human out of the loop."

they are controlled by pre-established algorithms, and conduct targeting operations according to predetermined scenarios, or when they are authorized or supervised by humans. At the other end of the continuum, cyber weapons are highly autonomous where they utilize adaptive intelligence and self-learning capabilities in their efforts to identify and engage targets in complex and dynamic environments and when there is no communication with a human agent once launched. Highly autonomous cyber weapons are thus self-governing. Although they operate within a framework of planned behavior, they are able to make independent decisions in response to external variables and by interacting with the external environment and these decisions are made on the basis of internal programming, information, processes, conditions, and constraints.

Stuxnet is a good example of such a weapon, even if it was not deployed during an armed conflict.[5] Stuxnet was a computer worm that was surreptitiously downloaded (probably through a compromised USB stick) onto the Intranet at the Natanz nuclear facility in Iran and it was designed to frustrate Iran's efforts to enrich uranium and develop nuclear energy. Operating within a complex web of interconnected networks, Stuxnet was able to identify specific models of programmable logic controllers (PLCs) manufactured by Siemens. These PLCs allowed the facility's computers to control the centrifuges used to enrich uranium. Stuxnet altered the PLCs' programming, which caused the centrifuges to spin too quickly and for too long. These changes prevented the enrichment of uranium and caused the physical destruction of a large number of centrifuges. To remain undetected, Stuxnet recorded sensor values during the period in which the PLCs were operating normally. Once enough data had been collected, Stuxnet modified the PLCs' programming while at the same time feeding computer operators fake sensor values, leading them to believe that the PLCs were functioning normally. An interesting feature of the Stuxnet virus was that, once deployed, it could not

---

Current autonomous weapons have varying degrees of autonomy. *See, e.g.*, Alan L. Schuller, *At The Crossroads of Control: The Intersection of Artificial Intelligence in Autonomous Weapon Systems with International Humanitarian Law*, 8 HARVARD NATIONAL SECURITY JOURNAL 379 (2017); PAUL SCHARRE & MICHAEL C. HOROWITZ, CENTER FOR A NEW AMERICAN SECURITY, AN INTRODUCTION TO AUTONOMY IN WEAPON SYSTEMS (2015), https://www.cnas.org/publications/reports/an-introduction-to-autonomy-in-weapon-systems.

5. For an overview of Stuxnet, see MARCO DE FALCO, NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, STUXNET FACTS REPORT: A TECHNICAL AND STRATEGIC ANALYSIS (2012), https://ccdcoe.org/library/publications/stuxnet-facts-report-a-technical-and-strategic-analysis-2/.

interact with its operators since, for security purposes, Natanz is an air-gapped facility insofar as it is not connected to the wider Internet.

When ACWs engage in operations that produce "acts of violence against the adversary," they qualify as "attacks" and must comply with the rules of international humanitarian law (IHL).[6] Grave or serious breaches of IHL constitute war crimes.[7] The question that immediately arises, and which will be considered in this article, is whether commanders can be held criminally liable for such crimes.

Commanders can be held criminally liable as perpetrators if they use an ACW to commit the actus reus of a crime with intent or knowledge.[8] For example, if a commander individually or jointly with others launches an ACW in order to kill protected civilians or is aware that such killings will occur in the ordinary course of events, they will be held responsible as perpetrators or co-perpetrators of the war crime of intentionally directing attacks against a civilian population.[9] Commanders also can be held criminally liable as perpetrators if they commit a war crime through another person; when, for example, they control the will of a person who goes on to commit a war crime by using ACWs.[10] Moreover, commanders can be held criminally liable as accomplices if they intentionally or with knowledge assist in the commission of a war crime by another person through the use of ACWs.[11]

All this may be possible when ACWs are used in clearly defined and well-structured operational environments against pre-planned and stable targets. However, where an ACW is deployed into a complex and evolving operational environment and has the capacity to make dynamic targeting decisions, it cannot be said that the commander intended the commission of a

6. *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 49(1), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

7. Rome Statute of the International Criminal Court art. 8, July 17, 1998, 2187 U.N.T.S. 90 [hereinafter Rome Statute].

8. *Id.* art. 25(3)(a) ("Commits such a crime, whether as an individual, jointly with another or through another person, regardless of whether that other person is criminally responsible."); *see also id.* art 30.

9. *Id.* art. 8(2)(b)(i).

10. *Id.* art. 25(3)(a) (addressing the perpetration of a crime through another person).

11. *Id.* art. 25 (3)(b)–(d).

war crime, that he or she had knowledge that it would occur, or that he or she assisted in its commission.[12]

In view of the above, in this article we consider an alternative form of liability attached by international criminal law to military commanders, namely, command responsibility.[13] Command responsibility is an indirect mode of liability that holds commanders criminally liable for their failure to prevent or repress crimes committed by their subordinates.[14]

In order to apply the law of command responsibility to ACWs, it is important to explain how we envisage the relationship between a commander and an ACW. This is because command responsibility is grounded on a human-to-human relationship, that is, the relationship between commanders and their subordinates (soldiers). This construction of command responsibility can certainly apply when, for example, soldiers commit war crimes by using ACWs and the commander fails to prevent their commission or fails to repress them.

However, our focus in this article is different: it is on the relationship between a commander and an ACW. We submit that the relationship between a commander and an ACW resembles and replicates the relationship between commanders and their soldiers. This is because ACWs are agents that operate within an organized system of command and control even if they act on their own when executing an order or have self-learning and adaptive capabilities. This system of command and control comprises resources (human and material), structures, facilities, processes (for example, training) and legal and military authority according to which commanders

12. This is particularly so since *dolus eventualis* (recklessness) has not been included within the ICC's mens rea requirements. *See* Prosecutor v. Lubanga, ICC-01/04-01/06-2842, Judgment, ¶ 1011 (Mar. 14, 2012).

13. Rome Statute, *supra* note 7, art. 28.

14. These crimes include genocide, crimes against humanity, war crimes, and the crime of aggression. It should be noted that command responsibility can run in parallel with direct forms of responsibility. According to existing jurisprudence, if both direct responsibility and command responsibility are established in relation to the same conduct, the former takes precedence and the position of the accused as commander is considered to be an aggravating circumstance when sentencing. *See* Prosecutor v. Blaskić, Case No. IT-95-14-A, Appeals Chamber Judgment, ¶¶ 91–92 (Int'l Crim. Trib. for the Former Yugoslavia July 29, 2004); Prosecutor v. Kajelijeli, Case No. ICTR-98-44A-A, Appeals Chamber Judgment, ¶ 81 (May 23, 2005); Prosecutor v. Kaing Guek Eav alias Duch, Case No. 001/18-07-2007/ECCC/TC, Judgment, ¶ 539 (July 26, 2010).

can exercise, maintain and actualize their command.[15] It allows commanders to manage resources; collect and assess information; plan operations; make decisions; direct and execute operations; supervise, monitor and assess operations, behaviors and actions; and take corrective action. It also ensures that operations are accomplished according to their objectives and within the law in circumstances of operational uncertainty, imperfect information and time-constraints. Operating within such a command and control system also means that the decision-making capacity and independence of subordinates is bounded and conditioned, albeit in different respects and to different degrees. It is because of the existence of this command and control system that ACWs can be considered subordinates. The relationship between commanders and ACWs is thus analogous to that of commanders and soldiers because soldiers operate within an organized system of command and control and are considered subordinates even if they are able to make independent decisions.[16]

It is also important to note that in both cases (soldiers and ACWs) commanders exercise macro-level command and control to ensure that their subordinates operate within the law and within their command as well as micro-level command and control to effectuate their command in particular circumstances or in relation to particular subordinates.[17] The two levels are interconnected, interdependent and integrated within the concept of command and control and it must be viewed holistically. To explain, while micro-command requires the application of the command and control tools to specific instances and persons, it can be exercised only if the framework of macro-level command and control is in place and functioning effectively. That said, the difference between exercising command and control over soldiers and ACWs lies in the fact that in the latter case command and control

15. *See* FRANK M. SNYDER, COMMAND AND CONTROL: READINGS AND COMMENTARY (1993); Loren D. Diedrichsen, *Command and Control: Operational Requirements and System Implementation*, 5 INFORMATION AND SECURITY 23 (2000); U.S. MARINE CORPS, MCDP 6, THE NATURE OF COMMAND AND CONTROL 33–60 (1996), https://www.marines.mil/Portals/1/Publications/MCDP%206%20Command%20and%20Control.pdf.

16. *See* Jens David Ohlin, *The Combatant's Stance: Autonomous Weapons on the Battlefield*, 92 INTERNATIONAL LAW STUDIES 1 (2016); Gary S. Corn, *Autonomous Weapons Systems: Managing the Inevitability of 'Taking the Man Out of the Loop'*, *in* AUTONOMOUS WEAPONS SYSTEMS: LAW, ETHICS, POLICY 209 (Nehal Bhuta, Susanne Beck, Robin Geiβ, Hin-Yan Liu & Claus Kreβ eds., 2016).

17. Prosecutor v. Halilović, Case No. IT-01-48-T, Judgment, ¶¶ 79–100 (Int'l Crim. Trib. for the Former Yugoslavia Nov. 16, 2005) (noting that the trial chamber speaks of a general and specific duty of a commander to prevent).

is exercised, maintained and achieved through technical means whereas in the case of soldiers it is achieved through interpersonal, physical, or institutional means.

Having explained the relationship between commanders and ACWs, we will now apply the law of command responsibility to this relationship. The article proceeds as follows. Part II introduces the doctrine of command responsibility and identifies its core elements, namely, the existence of a superior-subordinate relationship; the commission or prospective commission of crimes by subordinates; and the commander's knowledge or constructive knowledge of such crimes. Parts III through VII examine how these elements apply to ACWs, including a discussion of the scope of the element of causality introduced by Article 28 of the Rome Statute as well as the scope of responsibility of successor commanders. Part VIII concludes.

II. THE LAW OF COMMAND RESPONSIBILITY

The principle of command responsibility is well established in military doctrine and international criminal law.[18] It derives from the principle of responsible command,[19] according to which the commander, as the placeholder for the State, becomes the "guarantor" of IHL. For this reason, he or she is

18. *See* Prosecutor v. Mucić et al., Case No. IT-96-21-T, Judgment, ¶ 333 (Int'l Crim. Trib. for the Former Yugoslavia Nov. 16, 1998) [hereinafter Mucić, Judgment]; 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW r. 153, at 558–63 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005); *see generally* Mijan Damaska, *The Shadow Side of Command Responsibility*, 49 AMERICAN JOURNAL OF COMPARATIVE LAW 455 (2001); Kai Ambos, *Superior Responsibility*, *in* THE ROME STATUTE OF THE INTERNATIONAL CRIMINAL COURT: A COMMENTARY 823 (Antonio Cassese, Paola Gaeta & John R.W.D. Jones eds., 2002); GUÉNAËL METTRAUX, THE LAW OF COMMAND RESPONSIBILITY (2009); CHANTAL MELONI, COMMAND RESPONSIBILITY IN INTERNATIONAL CRIMINAL LAW (2010), Nicholas Tsagourias, *Command Responsibility and the Principle of Individual Criminal Responsibility: A Critical Analysis of International Jurisprudence*, *in* PROTECTING HUMANITY: ESSAYS IN INTERNATIONAL LAW AND POLICY IN HONOUR OF NAVANETHEM PILLAY 817 (Chile Eboe-Osuji ed., 2010); 1 KAI AMBOS, TREATISE ON INTERNATIONAL CRIMINAL LAW 197–232 (2013); THE ROME STATUTE OF THE INTERNATIONAL CRIMINAL COURT: A COMMENTARY 1056–1106 (Otto Triffterer & Kai Ambos eds., 3d ed. 2016).

19. *See* Regulations Respecting the Laws and Customs of War on Land art. 1(1), annexed to Convention No. II with Respect to the Laws and Customs of War on Land, July 29, 1899, 32 Stat. 1803, T.S. No. 403; Additional Protocol I, *supra* note 6, arts. 86–87; *see also* COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶¶ 3549–50 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987).

entrusted with powers to foster and ensure compliance with IHL. Importantly, a commander's dereliction of this duty attracts sanctions, including criminal ones.[20]

As an international criminal law principle, command responsibility was developed by war crimes tribunals, particularly after World War II.[21] It was later codified in the statutes of international criminal tribunals—specifically, Article 7(3) of the Statute of the International Criminal Tribunal for the former Yugoslavia (ICTY)[22] and Article 6(3) of the Statute of the International Criminal Tribunal for Rwanda (ICTR),[23] which contributed to the development of the doctrine. It has also been codified in Article 28 of the Rome Statute establishing the International Criminal Court (ICC).[24]

The three main constitutive elements of command responsibility as formulated in Article 28 of the Rome Statute are:

(i) The existence of a superior-subordinate relationship;
(ii) The superior knew or should have known that international crimes were about to be committed or had been committed by subordinates; and
(iii) The commander failed to take the necessary and reasonable measures to prevent or repress the commission of the crimes or to submit the matter to the competent authorities for investigation and prosecution.[25]

Article 28 also requires a causal nexus between the crimes and the commander's failure to exercise proper command.

How these elements apply to ACWs will be explored in the Parts that follow but, before this discussion, we need to explain the nature of command

20. Halilović, *supra* note 17, ¶¶ 39, 87; Prosecutor v. Bemba, ICC-01/05-01/08, Judgment, ¶ 172 (Mar. 21, 2016) [hereinafter Bemba, Judgment].

21. *See, e.g.*, United States v. Yamashita, 4 LAW REPORTS OF TRIALS OF WAR CRIMINALS 1 (1948); United States v. von Leeb et al. (The High Command Case), 11 TRIALS OF WAR CRIMINALS BEFORE THE NUREMBERG MILITARY TRIBUNALS UNDER CONTROL COUNCIL LAW NO. 10, at 542–45 (1950).

22. Statute of the International Criminal Tribunal for the former Yugoslavia art. 7(3), S.C. Res. 827 (May 25, 1993), adopting the Secretary-General Report Pursuant to Paragraph 2 of Security Council Resolution 808.

23. Statute of the International Criminal Tribunal for Rwanda art. 6(3), S.C. Res. 955 annex, (Nov. 8, 1994), *reprinted in* 33 INTERNATIONAL LEGAL MATERIALS 1598 (1994).

24. In its modern formulation, command responsibility encompasses both military and civilian superiors but this article focuses exclusively on military commanders.

25. Rome Statute, *supra* note 7, art. 28.

responsibility[26] because this will have a bearing on the interpretation of its elements.

Article 28 of the Rome Statute casts command responsibility as a mode of liability for the crimes of subordinates when it states that commanders are responsible "for" the crimes of their subordinates.[27] By contrast, the ad hoc tribunals treat command responsibility as responsibility for the dereliction of an affirmative duty to prevent or repress crimes committed by subordinates. As the ICTY trial chamber opined in *Halilović*:

> The Trial Chamber finds that under Article 7(3) command responsibility is responsibility for an omission. The commander is responsible for the failure to perform an act required by international law. This omission is culpable because international law imposes an affirmative duty on superiors to prevent and punish crimes committed by their subordinates. Thus "for the acts of his subordinates" as generally referred to in the jurisprudence of the Tribunal does not mean that the commander shares the same responsibility as the subordinates who committed the crimes, but rather that because of the crimes committed by his subordinates, the commander should bear responsibility for his failure to act. The imposition of responsibility upon a commander for breach of his duty is to be weighed against the crimes of his subordinates; a commander is responsible not as though he had committed the crime himself, but his responsibility is considered in proportion to the gravity of the offences committed.[28]

In our opinion, this is a better approach because it comports with the principle of culpability in that commanders bear responsibility for their own

---

26. *See* Ambos, *Superior Responsibility*, *supra* note 18; GERHARD WERLE & FLORIAN JESSBERGER, PRINCIPLES OF INTERNATIONAL CRIMINAL LAW 221–22 (2014); Chantal Meloni, *Command Responsibility: Mode of Liability for the Crimes of Subordinates or Separate Offence of the Superior?*, 5 JOURNAL OF INTERNATIONAL CRIMINAL JUSTICE 619 (2007); Darryl Robinson, *How Command Responsibility Got So Complicated: A Culpability Contradiction, Its Obfuscation, and a Simple Solution*, 13 MELBOURNE JOURNAL OF INTERNATIONAL LAW 1 (2012). On how command responsibility applies to cyber war, see TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS r. 85, at 396–400 (Michael N. Schmitt ed., 2017) [hereinafter TALLINN MANUAL 2.0].

27. Bemba, Judgment, *supra* note 20, ¶ 171. *Contra* Ambos, *Superior Responsibility*, *supra* note 18, at 851.

28. Halilović, *supra* note 17, ¶ 54; Prosecutor v. Hadžihasanović and Kubura, Case No. IT-01-47-T, Judgment, ¶¶ 74–75 (Int'l Crim. Trib. for the Former Yugoslavia Mar. 15, 2006) [hereinafter Hadžihasanović, Judgment]; Prosecutor v. Krnojelac, Case No. IT-97-25-A, Appeals Chamber Judgment, ¶ 171 (Int'l Crim. Trib. for the Former Yugoslavia Sept. 17, 2003).

culpable omissions concerning their subordinates' crimes rather than being criminally liable for these crimes themselves. Further, to treat command responsibility as a form of participation in the crimes of others undermines Article 25 of the Rome Statute or makes Article 28 irrelevant.[29] This approach also comports with the rationale of command responsibility which, as explained earlier, makes commanders guarantors of legality during an armed conflict, due not only to their powers, but also to the special relationship that exists between commanders and subordinates.

III. THE EXISTENCE OF A SUPERIOR-SUBORDINATE RELATIONSHIP

The first constitutive element of command responsibility is that of a superior-subordinate relationship which, in effect, refers to a command and control relationship.[30] This relationship can be de jure or de facto. The former refers to a commander's vested authority over subordinates,[31] with the military service being the primary institution operating under a formal command and control. Yet, a command and control relationship does not need to be formal. It can also arise from factual or other subordination circumstances, mainly due to a person's de facto authority and powers of control.[32] In this case, one can speak of a de facto commander.[33] However, the most decisive

29. Halilović, *supra* note 17, ¶ 78. Although command responsibility is often referred to as a *sui generis* mode of liability, see Bemba, Judgment, *supra* note 20, ¶ 174, it is not always clear to what this refers. But, according to van Sliedregt, command responsibility combines aspects of mode liability and aspects of separate offense liability. *See* ELIES VAN SLIEDREGT, INDIVIDUAL CRIMINAL RESPONSIBILITY IN INTERNATIONAL CRIMINAL LAW 196 (2012).

30. Prosecutor v. Limaj et al., Case No. IT-03-66-T, Judgment, ¶ 521 (Int'l Crim. Trib. for the Former Yugoslavia Nov. 30, 2005) (citation omitted)

> The superior-subordinate relationship lies at the heart of the doctrine of a commander's liability for crimes committed by [his or] her subordinates. It is the position of command over and the power to control the acts of the perpetrator which forms the legal basis for the superior's duty to act and for his [or her] corollary liability for a failure to do so.

31. Command has been defined as "[t]he authority that a commander in the armed forces lawfully exercises over subordinates by virtue of rank or assignment," whereas command and control has been defined as "[t]he exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission." Joint Chiefs of Staff, DOD Dictionary of Military and Associated Terms 40 (June 2020), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

32. Limaj, *supra* note 30, ¶ 522.

33. Command responsibility can thus extend to non-military superiors effectively acting as military commanders. *See* Prosecutor v. Mucić et al., Case No. IT-96-21-A, Appeals Chamber Judgment, ¶ 195 (Int'l Crim. Trib. for the Former Yugoslavia Feb. 20, 2001) [hereinafter Mucić, Appeals Chamber Judgment]; Prosecutor v. Bagilishema, Case No. ICTR 95-

factor is the commander's "effective command and control or authority and control" over subordinates.[34] This suggests a "real" or "actual power to control,"[35] which in the case of command responsibility refers to "the material ability to prevent or punish criminal conduct."[36] Put differently, effective control refers to the capacity of commanders to effectuate their command over subordinates in general or in particular circumstances. Whether this capacity exists in the particular circumstances is a matter of evidence and is assessed on a case-by-case basis, whereas the existence of de jure command only creates a rebuttable presumption of effective control.[37] That said, what the law requires is for the commander to have a functional command and control system.[38]

1A-A, Appeals Chamber Judgment, ¶ 35 (July 3, 2002); Bemba, Judgment, *supra* note 20, ¶¶ 176–77. This distinguishes them from civilian superiors as defined in Article 28(b) of the Rome Statute.

34. Bemba, Judgment, *supra* note 20, ¶ 189. The requirement of effective command and control is explicitly stated in Article 29 of the Law Establishing the Extraordinary Chambers in the Courts of Cambodia. Law on the Establishment of the Extraordinary Chambers in the Courts of Cambodia for the Prosecution of Crimes Committed During the Period of Democratic Kampuchea ch. VIII, art. 29, as amended by NS/RKM/1004/006 (Oct. 27, 2004) [hereinafter Law on the Establishment of the ECCC]. Although "command" and "authority" are deemed to refer to the same thing, one can say that "command" relates to de jure and "authority" to de facto commanders; *see also* Prosecutor v. Bemba, ICC-01/05-01/08-424, Decision Pursuant to Article 61(7)(a) and (b) of the Rome Statute on the Charges of the Prosecutor Against Jean-Pierre Bemba Gombo, ¶¶ 412–13 (June 15, 2009) [hereinafter Bemba, Decision Pursuant to Article 61(7)(a) and (b)].

35. Bemba, Decision Pursuant to Article 61(7)(a) and (b), *supra* note 34, ¶ 418; *see also* Prosecutor v. Kordić and Čerkez, Case No. IT-95-14/2-T, Judgment, ¶ 422 (Int'l Crim. Trib. for the Former Yugoslavia Feb. 26, 2001); Prosecutor v. Mucić et al., Case No. IT-96-21-T, Judgment, ¶ 370 (Int'l Crim. Trib. for the Former Yugoslavia Nov. 16, 1998); Mucić, Appeals Chamber Judgment, *supra* note 33, ¶ 256. "Effective control" for the purposes of command responsibility does not have the same meaning as in the law of State responsibility, which is about the State's effective control over a wrongful act. *See* G.A. Res. 56/83, annex, Responsibility of States for Internationally Wrongful Acts, art. 8 (Jan. 28, 2002). It is also different from the notion of control over the crime or over the will of the perpetrator, which is required for co-perpetration or for perpetration through another person according to the Rome Statute. Instead, effective control in the law of command responsibility is control over subordinates. Limaj, *supra* note 30, ¶ 522.

36. Limaj, *supra* note 30, ¶ 522; *see also* Bemba, Judgment, *supra* note 20, ¶ 183.

37. Mucić, Appeals Chamber Judgment, *supra* note 33, ¶ 197; Hadžihasanović, Judgment, *supra* note 28, ¶¶ 845–46.

38. It is important to stress that ad hoc command and control in relation to a particular instance is not equivalent to effective command and control as required by the law.

In *Bemba*, the ICC trial chamber noted a number of factors drawn from existing jurisprudence that may indicate the existence of effective command and control. These factors include:

> (i) the official position of commanders within military structures and the actual tasks they carried out;
> (ii) the power of the commander to issue orders, including his capacity to order forces or units under his command, whether under his immediate command or at lower levels, to engage in hostilities;
> (iii) the capacity to ensure compliance with orders, including consideration of whether the orders were actually followed;
> (iv) the capacity to re-subordinate units or make changes to command structure;
> (v) the power to promote, replace, remove, or discipline any member of the forces, and to initiate investigations;
> (vi) the authority to send forces to locations where hostilities take place and withdraw them at any given moment;
> (vii) independent access to, and control over, the means to wage war, such as communication equipment and weapons;
> (viii) control over finances;
> (ix) the capacity to represent the forces in negotiations or interact with external bodies or individuals on behalf of the group; and
> (x) whether the individual represents the ideology of the movement to which the subordinates adhere and has a certain level of profile, manifested through public appearances and statements.[39]

By contrast, the trial chamber explained that a lack of effective command and control can be indicated by a number of factors, namely:

> (i) the existence of a different exclusive authority over the forces in question;
> (ii) disregard or non-compliance with orders or instructions of the accused;
> (iii) a weak or malfunctioning chain of command; and
> (iv) the existence of intermediaries that prevent a commander from exercising effective command and control over subordinates.[40]

39. Bemba, Judgment, *supra* note 20, ¶ 188.

40. *Id.* ¶¶ 184, 190; *see also* Prosecutor v. Nuon Chea et al., Case No. 002/19-09-2007/ECCC/TC, Judgment, ¶¶ 1016–22 (Aug. 7, 2014).

It transpires that most of the aforementioned factors apply to ACWs which, as we said, operate within a system of command and control. In principle, a commander can issue orders to an ACW, direct or modify its operations, and supervise and monitor it to ensure compliance with IHL. A commander can also replace the weapons or withdraw them from the field.[41] Whether these powers amount to effective control depends on the weapon's programming, how it is designed to operate, and the extent to which its activities can be supervised and overridden by the commander. For example, algorithms may govern the activities of cyber weapons, restricting their attack capability to specific targets within certain networks and for a limited period. They can also strictly limit a weapon's area of operation or require it to comply with clearly defined rules of engagement. All these design and programming choices make its operation more deterministic and predictable.

Furthermore, ACWs may remain under the close supervision of a commander through a constant and real-time monitoring mechanism that allows him or her to adjust the algorithm to modify instructions, assign new tasks, or correct glitches. A commander may also have the ability to abort operations or deactivate a cyber weapon if it starts to behave unexpectedly or once it has successfully completed its mission. Under such circumstances, it is fair to conclude that the ACW acts under the effective command and control of the commander.

ACWs can, however, be driven by powerful algorithms that enable them to determine which targets to engage, when they should be engaged, how they should be engaged, whether the target has been neutralized or should be re-engaged, and when to proceed to the next task. Highly autonomous cyber weapons can make these decisions very quickly and relay back to the commander vast quantities of complex data,[42] all of which may effectively deprive a commander of his or her ability to supervise the weapon's activities or intervene when problems occur. Also, and as with the Stuxnet virus, ACWs may be deployed into private or secure networks, in which case the commander is unable to communicate with them. In such cases, the degree of effectiveness of a commander's control over ACWs can be questioned and needs to be proven on a case by case basis. It should also be remembered

41. Borrowing from the jurisprudence on "perpetration through another" due to an organized system of command and obedience, fungibility is evidence of the superior's power of control. *See* Prosecutor v. Katanga and Chui, ICC-01/04-01/07, Pre-Trial Chamber I Decision, ¶¶ 516, 518 (Sept. 30, 2008).

42. *See* CHRISTOPHER M. BISHOP, PATTERN RECOGNITION AND MACHINE LEANING (2006).

in this respect that the commander's duty to control is continuous and does not cease with the order or fielding of the weapon even if the ACW has been programmed appropriately.

The above scenario is different from where a subordinate disregards the orders or instructions of a commander. According to the ICC trial chamber in *Bemba*, the latter scenario describes a situation where effective control is lacking due to disobedience. When however an ACW acts differently than instructed, it is not because it refuses to follow orders or disregards orders, but because it executes the order differently due to the fact that it processes the information differently. In short, the order is still executed within the parameters of command and control. Even if a question arises regarding the commander's effective control over the weapon's processing function when crimes are committed, the circumstances and reasoning are different from those involved in a scenario of disobedience.

Disobedience is also different from a situation where an ACW selects and engages targets even if not specifically instructed by the commander but being consistent with the commander's instructions regarding the type of targets to be engaged and the circumstances under which they should be engaged. In this case, the targeting decisions by the ACW fall within the commander's framework of command and control but, depending on the circumstances, questions may arise about the degree of effective control over the ACW.

A scenario where effective control would be lacking is the case of a rogue AWC, that is, an ACW acting on its own initiative in order to pursue a goal outside of the framework of command.[43] In this instance, its actions fall outside of the commander's command and effective control and command responsibility cannot arise.

The role of intermediaries when determining the effectiveness of command and control was highlighted in the *Bemba* judgment,[44] and it is a critical issue when it comes to ACWs. One can say that programmers are intermediaries because they code ACWs prior to their deployment and will often need to update the weapons while they are operational. However, whether

43. Prosecutor v. Hadžihasanović and Kubura, Case No. IT-01-47-T, Appeals Chamber Judgment, ¶¶ 202–14 (Int'l Crim. Trib. for the Former Yugoslavia Apr. 22, 2008) [Hadžihasanović and Kubura, Appeals Chamber Judgment].

44. The trial chamber also distinguishes between the military principle of "unity of command" from effective command and control, with the former not precluding the existence of multiple commanders. *See* Bemba, Judgment, *supra* note 20, ¶¶ 698–99.

or to what extent they interrupt the effectiveness of command and control depends largely on whether they are integrated into the chain of command.

If they are integrated into the chain of command, the programmer's role is to support and enhance the commander's ability to exercise effective command and control by making ACWs operational and enabling the commander to be kept informed of their activities and to adjust them accordingly. It would require an exceptional set of circumstances for a programmers' input to be sufficiently substantial to interrupt the commander's effective command and control over an ACW. Similarly, it would be most unlikely that programmers who form part of the chain of command are able to exercise effective control over an ACW for the purpose of command responsibility because they do not plan the operation or, more specifically, they do not decide when the weapon will be deployed; which targets will be attacked and with what level of priority; what the weapon's overall objectives are; or when the weapon should be withdrawn. As international courts have consistently held, the exertion of mere influence—no matter how strong—does not equate to effective command and control.[45] It can thus be said that programmers integrated within the chain of command and operating in conformity with it do not interrupt its effectiveness. Integrating programmers into an effective command and control system may also be preferable. Otherwise, programming mistakes can reverberate to the command and control level and increase the risk of crimes being committed.

Programmers outside the chain of command can be treated as commanders themselves under certain circumstances. As we said, the law of command responsibility recognizes de facto authority and control. Moreover, effective command (or authority) and control does not mean exclusive command (or authority) and control.[46] In fact, the law of command responsibility recognizes parallel and multiple command structures in which responsibility is apportioned according to the level of control each person exercised at the relevant time. Thus, if a programmer controls how ACWs operate by feeding the system with predetermined operational scenarios, whereas the commander controls when and how these weapons are employed in the particular operation and relies without questioning on how the weapon has been programmed, it can be said that both exercise effective

45. *See, e.g.*, *id.* ¶ 183.
46. *Id.* ¶ 185.

command (or authority) and control over the weapon and can be held responsible under command responsibility providing the other requirements are met.

Such a situation would only arise in very exceptional circumstances when there is joint command and control by the operation commander and the programmer who makes the final programming decisions. It would not extend to manufacturers, developers, those responsible for authorising these weapons for military use or the programmers down the chain of programming. These individuals may be held accountable under different provisions or under domestic law, for example, under tort law but not under command responsibility because no effective command and control relationship as described previously exists between them and the weapon and no link exists with the particular crimes committed by the subordinates, which as we will explain below must be linked to how that command has been exercised.

IV. THE COMMANDER "KNEW" OR "SHOULD HAVE KNOWN"

According to Article 28(a)(i) of the Rome Statute, the commander must "either knew or, owing to the circumstances at the time, should have known that the forces were committing or about to commit such crimes."[47]

Knowledge primarily refers to actual knowledge established through direct or circumstantial evidence. Indices of knowledge include the number, type, and scope of illegal acts committed; the time during which they occurred; the number and type of troops involved; the logistics involved; the geographical location of the acts; their widespread occurrence; the tactical tempo of operations; the modus operandi of similar illegal acts; the officers and staff involved; and the location of the commander at that time.[48] Where knowledge is inferred, it must be the only reasonable inference even if it is not necessary to demonstrate that a commander knew about the specific crimes.

Consider a scenario where an ACW provides a commander with real-time reports on its activities and, in particular, informs the commander of which targets it has selected before it engages them. Where the cyber weapon proceeds to attack a civilian network, it can be reasonably inferred from the circumstances that the commander knew that a crime was about to be committed. By contrast, knowledge cannot be inferred where the ACW's reports

47. Rome Statute, *supra* note 7, art. 28(a)(i).
48. Mucić, Judgment, *supra* note 18, ¶ 386.

are incomplete, unintelligible, or unmanageable because of the size and complexity of the data being fed-back. Moreover, it may be the case that an ACW is able to select and engage a target incredibly quickly, perhaps in a matter of nanoseconds. Even if the ACW issues a report to the commander prior to targeting, the speed at which the target is actually engaged may make it difficult to conclude that the commander must have known that a crime was about to be committed. However, if the ACW reports back to the commander after the target has been engaged and it transpires that crimes have been committed, it can be said that the commander is aware that crimes have occurred.

Article 28 of the Rome Statute diverges from the ad hoc tribunals in relation to the second head of mens rea. According to the jurisprudence of the ad hoc tribunals, the commander must have "had reason to know" that the criminal act was about to be committed or had been committed, which means that some general "information was available to him which would have put him on notice of offences committed by subordinates."[49] Article 28 instead introduces a "should have known" standard that goes beyond the existence of notice and "requires more of an active duty on the part of the superior to take the necessary measures to secure knowledge of the conduct of his troops and to inquire, regardless of the availability of information at the time on the commission of the crime."[50] Consequently, a superior can be deemed "negligent in failing to acquire knowledge of his subordinates' illegal conduct."[51] It transpires from this that Article 28 introduces a mens rea of negligence by holding commanders responsible where they fail to apprise themselves of the behavior of their subordinates.[52]

---

49. Mucić, Appeals Chamber Judgment, *supra* note 33, ¶ 241; *see also* Hadžihasanović and Kubura Appeals Chamber Judgment, *supra* note 43, ¶ 28; Bagilishema, *supra* note 33, ¶ 42; Prosecutor v. Fofana and Kondewa, Case No. SCSL-04-14-T, Trial Chamber I Judgment, ¶ 233 (Special Court for Sierra Leone Aug. 2, 2007); *see also* Law on the Establishment of the ECCC, *supra* note 34, art. 29; 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 18, r. 153, at 558–63.

50. Bemba, Decision Pursuant to Article 61(7)(a) and (b), *supra* note 34, ¶ 433. The trial chamber did not deal with this issue. *See* Bemba, Judgment, *supra* note 20, ¶ 196.

51. Bemba, Decision Pursuant to Article 61(7)(a) and (b), *supra* note 34, ¶ 432.

52. Customary international law as determined by the ad hoc tribunals takes a contrary approach. *See* Mucić, Appeals Chamber Judgment, *supra* note 33, ¶ 226; Bagilishema, *supra* note 33, ¶¶ 32–37; Fofana and Kondewa, *supra* note 49, ¶ 245; Prosecutor v. Sesay, Kallon, and Gbao, Case No. SCSL-04-15-T, Judgment, ¶ 312 (Special Court for Sierra Leone Mar. 2, 2009).

When employing ACWs, it is important to stress that commanders cannot rely upon their lack of technological expertise to claim that they were not aware that crimes were about to be committed or had been committed.[53] The "should have known" standard envisages proactive commanders who familiarize themselves with their weapons' capabilities and limitations, which is what responsible command requires. At the same time, the "should have known" standard requires commanders to scrutinize the information presented to them by ACWs rather than treat it as immediately reliable and actionable. This addresses the risk of automation bias but, more than that, it does not invert the relationship between a commander and an ACW and does not effectively abolish the role of the commander.

Still, commanders are only expected to know what reasonable commanders should have known in their position.[54] Thus, where a cyber weapon is highly autonomous and is capable of sensing, learning, and adapting to new environments, it may not be reasonable to expect commanders to know that the weapon is about to commit a crime because it would be unreasonable to expect them to have known all situational variables and all the different ways they can be processed. Likewise, where the weapon operates in a private network, it may be difficult for a commander to predict how the weapon will react to this unknown environment or to discover that a crime was committed. That said, reasonable commanders would not deploy a weapon in an environment where they have no control over it, cannot reliably predict how it will act, or have not tested it.

A reasonable commander is also expected to keep up to date with the latest developments in technology. For example, imagine new software becomes available that enables an ACW to distinguish between military and civilian networks more accurately or to more precisely estimate the extent of collateral damage to civilian networks during an attack on military networks. Where commanders have this new technology available to them but fail to implement software upgrades, if a cyber weapon attacks civilian networks or causes excessive collateral damage, it could be said that a reasonable commander should have known that the outdated cyber weapon was prone (or at least more likely) to engage in criminal acts. Alternatively, commanders

53. TALLINN MANUAL 2.0, *supra* note 26, at 400 ("[T]he fact that cyber operations may be technically complicated does not alone relieve commanders or other superiors of the responsibility for exercising control over their subordinates. Willful or negligent failure to acquire an understanding of such operations is never justification for lack of knowledge.").

54. *Id.*

may give prior authorization for software updates to be installed automatically. If this is the case, commanders must place limits on the types of upgrades that can be automatically installed. In short, commanders must ensure that their authorization does not extend to updates that may compromise the weapon's ability to comply with IHL.

It may also transpire that an ACW has misdiagnosed a civilian network as a military network during a training exercise or when operating in the field. Technical reports may also surface that reveal the software used by the cyber weapon is defective. Similarly, media outlets or cyber security companies may independently report a weapon's defects, erratic behavior, vulnerabilities, or unauthorized conduct. Given that the information available to a commander need not be specific and must be viewed as a whole,[55] the commander in these circumstances "should have known" that crimes had been or were about to be committed.

We said above that under the "should have known" standard a commander has a positive duty to seek information and to scrutinize information, including that presented by the ACW. But what happens when, despite this, the commander comes to the wrong conclusion and crimes are committed? If the commander's assessment of the information was reasonable under the circumstances, the commander is exculpated. While the "should have known" criterion may impose a proactive duty upon the commander to inquire and find information, it is assessed on a case-by-case basis against material, temporal, and other related factors.

V. THE DUTY TO PREVENT OR REPRESS

Article 28 of the Rome Statute imposes three distinct duties on a commander: to prevent the commission of crimes, to repress crimes, or to submit the matter to the competent authorities for investigation and, if necessary, prosecution.[56] Existing jurisprudence, as developed mainly by the ad hoc tribunals, instead imposes on commanders a duty to prevent or punish. The duty to repress included in Article 28 can include the duty to punish and the duty to submit the matter to a competent authority.[57] For this reason, we will concentrate on the duty to prevent and the duty to repress. That said, it is important to make two points. The first point is that these duties should be

55. Prosecutor v. Krnojelac, Case No. IT-97-25-A, Appeals Chamber Judgment, ¶ 169 (Int'l Crim. Trib. for the Former Yugoslavia Sept. 17, 2003).

56. Rome Statute, *supra* note 7, art. 28(b)(iii).

57. Bemba, Judgment, *supra* note 20, ¶¶ 205–09.

viewed on a continuum and as a spectrum of particular duties rather than as alternatives.[58] The second point is that these duties are conditional; they are assessed against the criteria of necessity and reasonableness which, in turn, are assessed against the criterion of effective command and control.[59]

Necessary measures are those that are appropriate for the commander to take to discharge the duty to prevent or repress crimes and reasonable measures are those that fall within the commander's effective control.[60] The necessity and reasonableness of the measures are also assessed against the scope of the underlying crimes, the reliability of the available evidence, and the limitations presented when a commander is located some distance from where the crimes occur.[61] Moreover, whether the measures are necessary and reasonable does not necessarily depend on whether they were limited in "mandate, execution, and/or results."[62] Instead, they are dependent on whether any shortcomings were sufficiently serious, the commander was aware of them, it was materially possible to correct the deficiencies, and that they fell within the commander's authority to remedy.[63]

The duty to prevent spans the period from before the commission of crimes to their actual commission.[64] It comports with the general obligation to ensure respect for IHL[65] and the commander's special position and powers as a steward of IHL. To fulfill this duty, a commander must ensure that "forces are adequately trained in IHL; secure reports that military actions were carried out in accordance with IHL; issue orders aimed at bringing the relevant practices into accord with IHL; [and] take disciplinary measures to

58. Bemba, Decision Pursuant to Article 61(7)(a) and (b), *supra* note 34, ¶¶ 439–41.

59. Bemba, Judgment, *supra* note 20, ¶¶ 197–200; *see also* Harmen van der Wilt & Maria Nybondas, *The Control Requirement of Command Responsibility: New Insights and Lingering Questions Offered by the* Bemba *Appeals Chamber Case*, *in* MILITARY OPERATIONS AND THE NOTION OF CONTROL UNDER INTERNATIONAL LAW 327 (Rogier Bartels, Jeroen C. van den Boogaard, Paul A.L. Ducheine, Eric Pouw & Joop Voetelink eds., 2020).

60. Bemba, Judgment, *supra* note 20, ¶¶ 197–99; Hadžihasanović, Judgment, *supra* note 28, ¶¶ 121–28; Halilović, *supra* note 17, ¶¶ 79–100.

61. Prosecutor v. Bemba, ICC-01/05-01/08 A, Appeals Chamber Judgment, ¶¶ 183, 189 (June 8, 2018) [hereinafter Bemba, Appeals Chamber Judgment].

62. Bemba, Judgment, *supra* note 20, ¶ 720.

63. Bemba, Appeals Chamber Judgment, *supra* note 61, ¶¶ 180–01.

64. Bemba, Decision Pursuant to Article 61(7)(a) and (b), *supra* note 34, ¶ 437.

65. As set forth in Common Article 1 of the 1949 Geneva Conventions. *See, e.g.*, Convention (I) for the Amelioration of the Condition of the Wounded and Sick in the Armed Forces in the Field art. 1, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31.

prevent the commission of atrocities by the troops under the superior's command."[66] The commander must also: (i) issue orders specifically meant to prevent the crimes, as opposed to merely issuing routine orders; (ii) protest against or criticize criminal conduct; (iii) insist before a superior authority that immediate action be taken; (iv) postpone military operations; (v) suspend, exclude, or redeploy violent subordinates; and (vi) conduct military operations in such a way as to lower the risk of specific crimes or to remove opportunities for their commission.[67]

The above can very well apply to ACWs. First, a commander must take all reasonable steps to ensure that an ACW is programmed in such a way as to enable it to comply with IHL and with the objectives of the operation. This requires a commander to ensure, among other things, that the weapon has been tested and verified to operate as anticipated; is functional and reliable; is secure and protected from interference through anti-tamper mechanisms; has the required connectivity; is supported by a robust and resilient communication and information exchange system; is subject to spatial and temporal limitations; operates a "capture first" command mechanism; can be programmed to recognize a list of protected targets; gives warnings before launching attacks; and is subject to real-time supervision. This does not mean that commanders must test every aspect of the cyber weapon for defects, a near-impossible task given how many lines of code are written into computer algorithms.[68] Rather, commanders must take all necessary and reasonable measures to identify and resolve defects prior to deployment.

Moreover, a commander must be trained to use the weapon and be aware of its operational capabilities and limitations, which means that the commander must be able to respond to problems if they occur. Again, this does not mean that a commander must be able to predict every aspect of the weapon's behavior, which would be extremely difficult in the context of an autonomous weapon operating in a virtual domain.[69] Instead, what is required is that the commander has a sufficiently sound understanding of the weapon to be confident that its activities will conform to IHL and that he or she will be able to intervene if required.

---

66. Bemba, Decision Pursuant to Article 61(7)(a) and (b), *supra* note 34, ¶ 438.

67. Bemba, Judgment, *supra* note 20, ¶ 204.

68. Interview with Alan C. Schultz, Director, Laboratory for Autonomous Systems Research, U.S. Naval Research Laboratory (Jan. 28, 2016).

69. Interview with Leslie Pack Kaelbling, Learning and Intelligent Systems Group, Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology (Sept. 16, 2016).

Once deployed, if commanders become aware that ACWs are about to commit crimes, they must again take all necessary and reasonable measures to prevent that activity or repress it when it is ongoing. This may require the cyber weapon's algorithm to be recoded or, where this would be insufficient to prevent the criminal acts, the commander would be expected to deactivate the weapon. Time is an important factor here because cyber weapons—especially when operating autonomously—can process information and make decisions very quickly. The upshot is that commanders may not have the time to prevent the cyber weapon from acting. In addition, a commander may not be able to interact with an ACW where it is operating in a closed network. Here, there is no opportunity for a commander to adjust, override, or deactivate the weapon if problems arise. In these circumstances, it may be necessary and reasonable for the commander to inform the opposing party that a cyber weapon is operating on one of its networks and at risk of engaging in criminal behavior.

The duty to repress arises during ongoing crimes and after the commission of crimes.[70] It is also a broad duty; it can include criminal, disciplinary, or administrative measures or punishment, criminal prosecution, investigations, reporting to relevant authorities, or any other measure that can repress criminal activity. The ICC trial chamber in *Bemba* defined repress as to "put down," "subdue," "restrain," and to "keep or hold back."[71] This definition is important when this duty applies to non-human agents where some of the aforementioned actions are not applicable.

At a minimum, where an ACW commits a crime because of a design flaw, it is incumbent upon the commander to patch the defect, which may mean referring it to the programmer or military cyber command authorities for reassessment and reprogramming. If that is not possible or the defect cannot be corrected immediately, it would be necessary for the commander to remove the weapon from the field until it can be safely redeployed.

An interesting question is whether a commander is under a duty to repress when an ACW has committed a crime while under a previous commander's command and control. This scenario may arise in the case of ACWs because, given the interconnected nature of cyberspace, they can produce reverberating effects, and any crimes they commit may not become known until after the attack has been completed and a full technical assessment has been conducted.

---

70. Hadžihasanović, Judgment, *supra* note 28, ¶ 125; Bemba, Judgment, *supra* note 20, ¶ 206.

71. Bemba, Judgment, *supra* note 20, ¶ 205.

This hypothetical raises the specter of successor command responsibility. The Nuremberg Military Tribunal,[72] ad hoc tribunals,[73] and the ICC[74] have rejected this possibility because they require the commission of crimes by subordinates to coincide with the commander's exercise of command and control at the time the crimes were committed. It seems that existing jurisprudence takes a formal and time-limited approach to command and control. The causal link between the crimes and the commander's failure to exercise proper command required by Article 28 is another reason advocating against successor responsibility.[75]

In our opinion, the acceptance of successor command responsibility rests on the nature and purpose of command responsibility.[76] If command responsibility entails responsibility for subordinates' crimes, a successor commander cannot be held responsible for failing to repress crimes committed on another commander's watch. But as we argued in Part II, the better approach is to see command responsibility as responsibility for the dereliction of duty and, if the purpose of command responsibility is to ensure compliance with the law, a successor commander has a duty to repress past crimes. Thus, if a successor commander is aware that crimes have been committed by an ACW, he or she should reassess, reprogram, or decommission the weapon, or request others to do so. Otherwise, time-limiting the commander's duty undermines IHL and the aims of command responsibility. If the commander fails to do so and uses the same cyber weapon, this would amount to dereliction of the duty to prevent further crimes.[77] And, if war crimes are indeed committed, he or she could be charged as a perpetrator or

72. United States v. von Leeb et al., *supra* note 21, at 1230.

73. Prosecutor v. Hadžihasanović and Kubura, Case No. IT-01-47-AR72, Decision on Interlocutory Appeal Challenging Jurisdiction in Relation to Command Responsibility, ¶ 51 (Int'l Crim. Trib. for the Former Yugoslavia July 16, 2003); Prosecutor v. Orić, Case No. IT-03-68-A, Appeals Chamber Judgment, ¶ 167 (Int'l Crim. Trib. for the Former Yugoslavia July 3, 2008) [hereinafter Orić, Appeals Chamber Judgment]; *see also* Christopher Greenwood, *Command Responsibility and the* Hadžihasanović *Decision*, 2 JOURNAL OF INTERNATIONAL CRIMINAL JUSTICE 598 (2004).

74. Bemba, Decision Pursuant to Article 61(7)(a) and (b), *supra* note 34, ¶ 419 ("[T]he Chamber is of the view that according to article 28(a) of the Statute, the suspect must have had effective control *at least* when the crimes were about to be committed.").

75. Ambos, *Superior Responsibility*, *supra* note 18.

76. Barrie Sander, *Unraveling the Confusion Concerning Successor Superior Responsibility in the ICTY Jurisprudence*, 23 LEIDEN JOURNAL OF INTERNATIONAL LAW 105 (2010).

77. Hadžihasanović and Kubura, Appeals Chamber Judgment, *supra* note 43, ¶¶ 30–31; Prosecutor v. Orić, Case No. IT-03-68-T, Judgment, ¶ 326 (Int'l Crim. Trib. for the Former Yugoslavia June 30, 2006) [hereinafter Orić, Judgment].

accomplice since, as noted in Part II, command responsibility and individual criminal responsibility apply in parallel.

An alternative situation where successor command responsibility can arise is when an ACW is deployed while under the effective command and control of a former commander but its violent effects are not felt until a later point because its activation is time-delayed, as would be the case with a logic bomb (a logic bomb is a piece of code that is surreptitiously inserted into computer software and a malicious function is triggered when specified conditions are met). If a successor commander becomes aware of the weapon's deployment and knows that, once activated, it will result in the commission of a crime, he or she should take all necessary and reasonable steps to prevent its activation. If the commander only becomes aware of the weapon after it has been activated and crimes have occurred, the duty to repress would be triggered, as previously discussed.

VI. CAUSALITY

According to Article 28 of the Rome Statute, crimes must be committed "as a result" of the superior's failure to exercise proper control.[78] Article 28, therefore, seems to introduce causality into the doctrine of command responsibility in contrast to the ad hoc tribunals that have rejected causality.[79]

Even if Article 28 requires causality, it does not provide much clarity as to its scope. For example, commanders cannot be said to "cause" subordinates to commit crimes where they fail to repress[80] or report the matter to a competent authority. This points to treating command responsibility as responsibility for dereliction of duty rather than as responsibility for participation in subordinates' crimes. Causality may, however, be relevant in relation to the duty to prevent. But how can a commander's failure cause a crime of intent, such as genocide, where the applicable mens rea is the "should have known" standard?

Another difficulty concerns the required standard of causation. In *Bemba*, the ICC trial chamber said that the "but for" test is such a threshold but not

78. Rome Statute, *supra* note 7, art. 28(a)–(b).

79. Mucić, Judgment, *supra* note 18, ¶¶ 398–400; Blaskić, *supra* note 14, ¶ 77; Halilović, *supra* note 17, ¶ 78; Hadžihasanović and Kubura, Appeals Chamber Judgment, *supra* note 43, ¶ 40; Orić, Judgment, *supra* note 77, ¶ 338. Moreover, no causality is required by the Law on the Establishment of the ECCC. *See supra* note 34.

80. Bemba, Decision Pursuant to Article 61(7)(a) and (b), *supra* note 34, ¶ 424; Mucić, Judgment, *supra* note 18, ¶ 400; Orić, Judgment, *supra* note 77, ¶ 338.

the only one.[81] Other judges established a causal link because of the "high probability" that crimes would not have been committed had the commander discharged his or her duty to prevent.[82] By contrast, other judges dismissed the need for a causal link altogether.[83]

In our view, if causation is an element of command responsibility, it is ingrained in the notion of effective command and control. This is because in order to establish the commander's failure to exercise proper control, what needs to be established first is that the commander had effective command and control and, as we said previously, this includes the ability to prevent or repress. Consequently, the commander's failure to fulfill his or her duty to prevent or repress when the material ability existed indicates a lack of proper control and links the commander to the underlying crime. Put differently, it is an objective causality proved by the commander's failure to prevent or repress without needing to also prove why the failure to exercise proper control could cause the crimes.[84] This approach is closer to the approach taken by the ad hoc tribunals and comports with what we said in the introduction that macro- and micro-command are interconnected, interdependent, and integrated, and therefore cannot be separated.[85] It also comports with our approach to command responsibility as responsibility for dereliction of duty.

---

81. Bemba, Judgment, *supra* note 20, ¶ 213.

82. *Id.* ¶ 24 (separate opinion of Steiner, J.); Bemba, Appeals Chamber Judgment, *supra* note 61, annex 2, ¶ 339 (dissenting opinion of Monageng J., and Hofmanski J.).

83. *Id.* annex 2, ¶¶ 55–56 (separate opinion of Van Den Wyngaert, J., and Morrison, J.).

84. The French version of Article 28(a) of the Rome Statute seems to comport with this interpretation:

> Un chef militaire ou une personne faisant effectivement fonction de chef militaire est pénalement responsable des crimes relevant de la compétence de la Cour commis par des forces placées sous son commandement et son contrôle effectifs, ou sous son autorité et son contrôle effectifs, selon le cas, *lorsqu'il ou elle n'a pas exercé le contrôle qui convenait sur ces forces* . . . .
>
> [A military commander or a person effectively acting as a military commander is criminally responsible for crimes within the jurisdiction of the Court committed by forces under his effective command and control, or under his effective authority and control, as the case may be, *when he or she has not exercised proper control over those forces*. . . .]

(emphasis added).

85. This also means that, as we have argued, the failure to exercise control properly and the failure to prevent or repress are interrelated and do not constitute two separate elements that need to established individually. *Contra* Separate Opinions of Judge Steiner and Judge Ozaki in Bemba, Judgment, *supra* note 20, annex I and II respectively. According to another approach, there is no causality but "as a result" refers to the responsibility of the commander for his or her omission. *See* Amnesty International, Amicus Curiae Observations on Superior Responsibility Submitted Pursuant to Rule 103 of the Rules of Procedure and Evidence ¶¶ 39–40, Doc. No. ICC-01/05-01/08-406 (Apr. 20, 2009).

What this means in the case at hand is that if a commander detects, for example, a code malfunction but fails to correct it, a causal link with any committed crimes is established because he or she did not exercise command properly by preventing the crimes.

VII. CRIMES COMMITTED

Under Article 28 of the Rome Statute, commanders are held criminally responsible under command responsibility for failing to prevent or repress the crimes committed by their subordinates. Therefore, it is important to explain what the term "crimes committed" means in the context of Article 28,[86] and whether ACWs operating under a system of effective command and control can commit crimes. These questions interrelate and will be considered in tandem. It is important to stress however that this question is different from the question of whether subordinates can be held criminally responsible. Command responsibility is triggered when crimes are being committed or have been committed and not when subordinates are held criminally responsible for these crimes. This is a crucial distinction to be made and it has implications for ACWs to the extent that they cannot be held criminally responsible because they are not moral agents.

One approach to the issue is to say that a crime is committed when both its actus reus and mens rea are present.[87] An ACW can commit the actus reus of a crime, for instance, by directly targeting a civilian network. The immediate question is whether they can have the requisite mens rea, which, as we noted, is intent or knowledge. Article 30(3) of the Rome Statute defines knowledge as an "awareness that a circumstance exists or a consequence will occur in the ordinary course of events."[88] An ACW can be aware of a circumstance where it is sensed or recognized. Because ACWs are aware of their capabilities, they can also be aware of the consequences of their actions; for example, they can be aware that a target will be destroyed if an order is executed. Moreover, ACWs that possess self-learning capabilities can learn from experience or "trial and error" and use this information to enrich and adjust their knowledge and actions. It can thus be concluded that ACWs can have ingrained as well as acquired knowledge.

86. THE ROME STATUTE OF THE INTERNATIONAL CRIMINAL COURT: A COMMENTARY, *supra* note 18, at 1088–89.

87. Williamson v. Norris [1899] 1 Q.B. 7, 14 (Eng. and Wales).

88. Rome Statute, *supra* note 7, art. 30(3).

ACWs can also fulfill the mens rea of intent in relation to consequences, which Article 30(2)(b) of the Rome Statute defines as awareness that consequences "will occur in the ordinary course of events."[89] Evidently, there is an overlap between the mens rea of intent and the mens rea of knowledge in relation to consequences. Regarding the required level of certainty, the ICC requires virtual certainty.[90] Virtual certainty is not absolute certainty which does not exist even in human reasoning. Virtual certainty means that any uncertainty that lingers is non-consequential. It follows from this that, depending on how they are programmed to reduce uncertainty, ACWs can have virtual certainty. For instance, when they attack a particular target in order to destroy it, they are certain of the consequences because they have been pre-determined in their coding whereas if doubt has been coded, they can abstain from acting because they are able to recognize the resulting consequences.

According to another approach, to commit a crime means the commission of a proscribed act.[91] A crime as a legally wrongful act[92] can be decoupled from the notion of culpability (mens rea), which is about attributing the unlawful act to a moral agent due to their personal stance toward that act. What makes the act wrongful and legally proscribed is its harmful actus reus (with harm not necessarily being physical), rather than its attribution to a moral agent. It follows from this that the underlying crime for command responsibility purposes is an objective circumstance that is established where the actus reus—or aspects of the actus reus—that condition a crime are present. According to this view, ACWs can fulfill the objective elements of a crime, for example, where they directly target civilian networks, a wrongful act in itself.

In our opinion, this is a better approach and one supported by a number of other considerations. First, the commander does not need to know the specificities of the crimes or the perpetrators' identities other than in general

89. *Id.* art. 30(2)(b).

90. Prosecutor v. Katanga, ICC-01/04-01/07, Judgment, ¶ 777 (Mar. 7, 2014).
Thus, this form of criminal intent presupposes that the person knows that his or her actions will necessarily bring about the consequence in question, barring an unforeseen or unexpected intervention or event to prevent its occurrence. In other words, it is nigh on impossible for him or her to envisage that the consequence will not occur.

91. Orić, Judgment, *supra* note 77, ¶ 296 (referring to the prosecution brief).

92. Glanville Williams, *The Definition of a Crime*, 8 CURRENT LEGAL PROBLEMS 107 (1955).

terms as being his or her subordinates.[93] Moreover, the obligation to prevent requires action before the commission of a crime while it is unfolding. Even when a commander suspects that a crime is about to be committed, he or she must intervene.[94] Also, the obligation to repress includes a duty to investigate or institute criminal proceedings that will eventually establish the facts and possibly the culpability. This means that command responsibility can be activated even if not all the elements of a crime have been fulfilled; and of course, if individuals do not have to be identified, mens rea cannot be established. Instead, what activates the commander's duty to act in these circumstances is the existence of acts that condition the commission of a crime.

Second, in order to enhance the effectiveness of command responsibility, international jurisprudence has not only applied it to all modes of perpetration or participation included in Article 25 (3)(a)–(f) of the Rome Statute,[95] but to inchoate crimes as well.

Third, command responsibility still attaches in situations involving exculpatory circumstances. For example, where a subordinate engages in a wrongful act, for example, killing civilians, but does not have the requisite mens rea due to an exculpatory circumstance such as mental impairment, command responsibility will attach if the commander failed to prevent or repress the killing. This outcome can be contrasted with the case where the act's wrongful character is removed because of a justification, for example, where a civilian is killed in self-defense. In this case, there is no wrongful act, and a commander cannot incur responsibility for his or her failure to prevent or repress what is a justifiable act.

Fourth, and most importantly, this approach accords with the nature of command responsibility as responsibility for the dereliction of duty rather than responsibility for the crimes of subordinates and comports with its rationale, which is to ensure that violations of IHL are prevented and repressed.

VIII. CONCLUSION

ACWs are likely to become a central feature of contemporary armed conflict. No technology is fail-safe and the question that arises is who can be held responsible if an ACW commits a war crime. This article has addressed this

93. Orić, Appeals Chamber Judgment, *supra* note 73, ¶ 35; Bemba, Judgment, *supra* note 20, ¶ 194.

94. Hadžihasanović, Judgment, *supra* note 28, ¶ 852.

95. Orić, Judgment, *supra* note 77, ¶¶ 294, 295–306, 328.

question from the perspective of the doctrine of command responsibility by placing ACWs within a system of command and control. It then explained how its constituent elements, as they have been interpreted in international jurisprudence, apply to ACWs. A number of questions have been raised in this context. To what extent does the autonomous nature of cyber weapons preclude commanders from exercising effective command and control over them? What is the role of intermediaries such as programmers, and do they interfere with the effectiveness of a commander's control over ACWs? Do successor commanders have command responsibility?

As we move along the autonomy continuum, when can it be said that a reasonable commander knew or should have known that an ACW was about to commit or had committed a crime? What necessary and reasonable measures must commanders take to discharge their duty to prevent or repress? Can ACWs commit a crime for the purpose of command responsibility?

In addressing these questions, it became clear that the law of command responsibility can apply to ACWs with the necessary adjustments and interpretative refinement. However, this legal framework faces serious challenges as one moves toward the upper echelons of autonomy. As autonomous technology advances, it is essential to determine how it can be made compatible with legal principles and demands for accountability. We believe that being human-made technology there is an opportunity to develop autonomous technology responsibly and to align it with the principles and aims of humanitarian law and international criminal law. In our view, the doctrine of command responsibility represents an important and powerful tool for ensuring that international law remains in the loop when ACWs are used.