Catholic University Journal of Law and Technology

Volume 29
Issue 2 *Spring 2021*

Article 3

2021

Brain-Computer-Interfacing & Respondeat Superior: Algorithmic Decisions, Manipulation, and Accountability in Armed Conflict

Salahudin Ali

BRAIN-COMPUTER-INTERFACING & RESPONDEAT SUPERIOR: ALGORITHMIC DECISIONS, MANIPULATION, AND ACCOUNTABILITY IN ARMED CONFLICT

Salahudin Ali[*+]

[*] Major Salahudin Ali is a commissioned officer and judge advocate in the United States Marine Corps. He received his LL.M. in 2018 from the Scalia School of Law at George Mason Univ.; and Juris Doctorate from the Lewis & Clark Law School in 2011. The comments, thoughts, and opinions in this article are those of the author and are not necessarily associated with the Department of Defense or any other government agency.
[+] The author recognizes that the existence of classified sources may significantly impact this article's analysis. All errors are my own.

"Nothing is at last sacred but the integrity of your own mind."-Ralph Waldo Emerson

"To understand the immeasurable, the mind must be extraordinarily quiet." - Jiddu Krishnamurti

I. SCIENCE FICTION TO REALITY.

Cybernetic technology has now entered the commander's brain.[1] In a viral online video produced by Naval Weapons Station China Lake, a hive of mind-controlled drones acts as a single organism upon intuitive command of a human operator by reading and interpreting his brain signals—the hive of drones were shown to support traditional military tactics by adapting to the users' tactics, predicting his intent.[2] As interesting as this new technology may be, there was no discussion as to the culpability or liability of the operator should something go wrong (although some organizations voiced concerns).[3]

This type of technology and its ability to enter the brain is not limited in its development to the military. For instance, Elon Musk's announcement of a new iteration of a wireless implants, produced by Neuralink, allows the brain to directly interface with digital devices, serving as a realization of previous "cyberpunk" technology.[4] Neuralink's technology, however, remains immature,

---

1 *Cybernetics*, MERRIAM-WEBSTER DICTIONARY, https://www.merriam-webster.com/dictionary/cybernetics (last visited May 17, 2021) (defining "Cybernetics" as "the science of communication and control theory that is concerned especially with the comparative study of automatic control systems [such as the nervous system and brain and mechanical-electric communication systems]").

2 Dep't of Def., *The Drone Swarm*, YOUTUBE (May 25, 2017), https://www.youtube.com/watch?v=0RHmA5eH-d4; *see also* Nita Farahany, *LENS 2018: Complexity & Security*, YOUTUBE (Feb. 23, 2018), https://www.youtube.com/watch?v=GS1IOjME5mA (Professor Farahany's presention at Duke's Center on Law, Ethics and National Security (LENS) annual national security conference).

3 *See* Thomas Gibbons-Neff, *Watch the Pentagon's New Hive-Mind-Controlled Drone Swarm in Action*, WASH. POST (Jan. 10, 2017), https://www.washingtonpost.com/news/checkpoint/wp/2017/01/10/watch-the-pentagons-new-hive-mind-controlled-drone-swarm-in-action/; Sam Bocetta, *What Are the Security Implications of Elon Musk's Neuralink?*, CSO ONLINE (Aug. 1, 2019), https://www.csoonline.com/article/3429361/what-are-the-security-implications-of-elon-musks-neuralink.html.

4 *See* Adam Rogers, *Neuralink Is Impressive Tech, Wrapped in Musk Hype*, WIRED

with many limitations such as the brain's natural and intolerable environment to foreign objects placed within it, physiological effects to the human brain, and resiliency in its operability.[5] These capabilities, developed by the private and public sectors, may be present in future kinetic combat action.[6]

The advent of these technologies raises serious legal questions in the context of accountability of use in combat operations where matters of life and death are inevitable. Legal tradition provides that actions which have kinetic affects are imparted on the humans who make them.[7] It is essential to a functional civilized society that humans are held accountable if such actions resulting in kinetic affects breach established legal regimes of liability and criminality.[8] This standard applies regardless of whether such actions are intentional or unintentional.[9] This is because the taking of life is primarily a human endeavor; regardless of the tool or platform, the decision point rests with a human.[10] The mental standards established by these legal regimes hold humans accountable due to the evolutionary concept of scienter, which require a requisite awareness of a given situation and a positive act to resolve it.[11] In other words, humans act with a level of control over their mental state to make such decisions in which they can foresee a consequence.[12]

Nowhere is the concept of accountability and culpability more important than

---

(Sept. 4, 2020), https://www.wired.com/story/neuralink-is-impressive-tech-wrapped-in-musk-hype/.

5 *See id.*

6 *See, e.g.*, Greg Allen, *Understanding AI Technology*, JOINT A.I. CTR. (Apr. 2020), https://www.ai.mil/docs/Understanding%20AI%20Technology.pdf (The DoD AI Strategy defines AI as ". . . the ability of machines to perform tasks that normally require human intelligence. . . . This definition includes decades-old DoD AI, such as aircraft autopilots, missile guidance, and signal processing systems. . . . Though many AI technologies are old, there have been legitimate technological breakthroughs over the past ten years that have greatly increased the diversity of applications where AI is practical, powerful, and useful.").

7 *See* LARRY ALEXANDER, OXFORD HANDBOOK OF JURISPRUDENCE AND PHILOSOPHY OF LAW, 819–20, 822 (Jules Coleman et al. eds., 2002).

8 *See id.* at 815–22.

9 *See id.* at 823.

10 *See* Alan L. Schuller, *At the Crossroads of Control: The Intersection of Artificial Intelligence in Autonomous Weapon Systems with International Humanitarian Law*, 8 HARV. NAT'L SEC. J. 379, 388–89 (2017).

11 *See* ALEXANDER, *supra* note 7, at 823–31 ("In order to be a culpable act, an act must be voluntary. If that were not the case…there would be no reason to exempt [a person] from criminal liability. A separate requirement that a voluntary act be proved is included within the requirement that a culpable act be proved"); *see also Scienter*, BLACK'S LAW DICTIONARY (2nd ed. 1910) (defining the word as "knowingly").

12 *See* Yavar Bathaee, *The Artificial Intelligence Black Box and The Failure of Intent and Causation*, 31 HARV. J.L. & TECH. 890, 906, 912 (2018).

in matters of unlawfully causing death.[13] In war, death is inevitable.[14] The concept of accountability and culpability for unlawful death in armed conflict is found in the Law of Armed Conflict (LOAC), which holds commanders or other superiors accountable for their own actions, as well those actions committed by troops under their charge that are not in compliance with established limitations and prohibitions on unlawful death.[15] This culpability and accountability regime is extended to platforms and weapons through command and control systems that resemble traditional human-to-human control; this is especially true where there are well-defined and static targets, clear objectives, a structured operational environment, and an uninterrupted or unaltered communication and execution of orders.[16] This LOAC concept is known as *respondeat superior* (also known as command responsibility).[17]

Generally, LOAC's primary purpose is meant to mitigate the destructive results of armed conflict, as well as the impacts on those who are not participants in such armed conflict.[18] LOAC achieves this through a myriad of signed agreements and normative, customary behaviors.[19] The general principles provided for destructive actions are that targets may be acquired, targeted, and destroyed if they meet criteria of being a military necessity; they are distinctively

---

13 Thomas E. Ricks, *What Ever Happened to Accountability?*, HARV. BUS. REV. (Oct. 2012), https://hbr.org/2012/10/what-ever-happened-to-accountability.

14 *Id*.

15 *See* GARY SOLIS, THE L. OF ARMED CONFLICT: INT'L HUMANITARIAN L. IN WAR 417–18 (Cambridge Univ. Press ed., 2nd ed. 2016); TALLINN MANUAL 2.0 ON THE INT'L L. APPLICABLE TO CYBER OPERATIONS, INT'L GRPS. OF EXPERTS AT THE INVITATION OF THE NATO COOP. CYBER DEF. CTR. OF EXCELLENCE 396–97 (Michael N. Schmitt & Liis Vihul eds., 2017) [hereinafter "TALLINN MANUAL 2.0"].

16 *See* SOLIS, *supra* note 15, at 417–18; *see also* Russell Buchan & Nicholas Tsagourias, *Autonomous Cyber Weapons and Command Responsibility*, 96 INT'L. L. STUD. 645, 648–49 (2020). ("[Culpability] may be possible when [autonomous weapons] are used in clearly defined and well-structured operational environments against pre-planned and stable targets. However, where an [autonomous weapon] 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 war crime, that he or she had knowledge that it would occur, or that he or she assisted in its commission.").

17 *See* SOLIS, *supra* note 15, at 417–18.

18 *See* THE JAG LEGAL CTR. & SCH., 2020 OPERATIONAL L. HANDBOOK 9 (U.S. Army, Micah Smith et al. eds., 2020).

19 Salahudin Ali, *Coming to a Battlefield Near You: Quantum Computing, Artificial Intelligence, & Machine Learning's Impact on Proportionality*, 18 SANTA CLARA J. INT'L L. 1, 4–5 (2020) (stating that, "In war, [] principles and standards of practice are governed by a complex set of normative behavior and signed agreements reflected in the law of armed conflict and customary international law"); *see also* Maj. Aaron L. Jackson & Col. Kristin D. Kuenzli, *Something to Believe In: Aligning The Principle Of Honor With the Modern Battlefield*, 6 NAT'L SEC. L.J. 35, 41 (2018) (stating that, "[LOAC] is not a singular work of art, but rather, a puzzle formed by hundreds of individual pieces of international and domestic law").

military in nature; destruction is proportionate in regard to actors and objects not involved in the conflict; such destruction does not result in unnecessary suffering; and targeting and destruction is conducted with a level of honor.[20] These principles are used as a guide to ensure that a commander or other superiors' decisions to take action, or the ordering of subordinates to take action which results in the loss of life, are based upon more than speculation, bias, recklessness, or in worst circumstances, a superfluous quest for death.[21] Indeed, many cases have demonstrated the proposition that commanders will not escape criminal liability for their own actions, nor will they escape liability for those actions conducted by subordinates they control when there is a failure of accountability for actions seen or unforeseen which violate the LOAC.[22]

As with any discipline, emerging technology serves as a disrupter.[23] An example of this can be found in the evolving nature of warfare, which now includes information operations, cyber operations, cybersecurity, use of autonomous and semi-autonomous systems, robotics, and many other developing aspects.[24] Recently, such discussion has focused on the role of human decision- making in the deployment of emerging technologies and as to what role humans should play within the decision cycle of autonomous platforms who act as agents or extensions of a decision maker.[25] The discussion is now more appropriately focused on cerebral and neurological process of decision-making reserved for humans and one emerging technology's ability to interfere or control such decision-making capacity known as Brain-Computer-Interfacing (BCI).[26] BCI enables users to externally and spatially interact with

---

20 Ali, *supra* note 19, at 5–6.

21 *Id.* at 6–7; Michael N. Schmitt & Jeffrey S. Thurnher, *"Out of the Loop": Autonomous Weapon Systems and the Law of Armed Conflict*, 4 HARV. NAT'L SEC. J. 231, 231–33, 253–58 (2013).

22 *See* SOLIS, *supra* note 15, at 427–33 n. 56–86 ("*Respondeat superior* is a broad concept, but its reach is not unreasonable. It must be accentuated that command responsibility is all about dereliction of duty. [The point is that] [t]he commander is held accountable for his own act [or omission], rather than incurring 'vicarious liability' for acts' for acts . . . of subordinates.").

23 Ali, *supra* note 19, at 1–2, 4 (2020).

24 *See* ANDREW FEICKERT ET AL., CONG. RES. SERV., U.S. GROUND FORCES ROBOTICS AND AUTONOMOUS SYS. AND ARTIFICIAL INTELLIGENCE: CONSIDERATIONS FOR CONG. 16 (2018); *see also* Lt. Col. Wilson C. Blythe Jr. & Lt. Col. Luke T. Calhoun, *How We Win the Competitions for Influence*, 99 MIL. REV. 37, 41, 45–46 (2019).

25 *See* Schuller, *supra* note 10, at 379, 386, 388; *see also* Buchan & Tsagourias, *supra* note 16, at 645, 648–50 (discussing the concept known as "humans in the loop").

26 Alexandre Gonfalonieri, *A Beginner's Guide to Brain-Computer Interface and Convolutional Neural Networks*, TOWARDS DATA SCI. (Nov. 25, 2018), https://towardsdatascience.com/a-beginners-guide-to-brain-computer-interface-and-convolutional-neural-networks-9f35bd4af948 (noting that other nomenclature exists regarding BCI neural-control interface [NCI]; Mind-machine interface [MMI]; direct neural interface [DNI]; or Brain-machine interface [BMI]).

computers and tools by means of brain-activity only, which are measured, processed, and controlled by a variety of technologies.[27] With the complexity of the system architecture, its use of artificial intelligence algorithms, its use of machine learning, and its signals acquisition processing, the discussion now shifts focus as to what place platforms take within a human's decision cycle as a cybernetic extension used to control subordinates or platforms, and what becomes of culpability and liability in such control.[28] This raises questions as to how decisions remain within the jurisdiction of a commander's mind? How mental assurance requirements will be met under LOAC regimes? How accountability will be had? What mental lines of departure exists for actions rising to criminal culpability?

II. ROADMAP.

Using LOAC as a guide, this article seeks to provide a foundation to answer questions and provide recommendations to facilitate a discussion as to how commanders, or those deemed superiors, may retain cognitive and intuitive freedom, allowing a level of responsibility and accountability for their actions. This in turn promotes compliance with established legal regimes regarding respondeat superior in the legal tradition of the LOAC. Indeed, results of previous cases dealing with respondeat superior may have differed if a technology such as BCI was available at the time. Through this article's discussion, recommendations such as cognitive liberty, retaining jurisdiction of the mind, and ethical algorithm design and architecture, may assist in limiting the impacts of BCI's inevitable arrival on the battlefield. A potential resolution of these issues may have consequences far beyond the niche field of LOAC, touching upon greater questions of culpability and accountability that society will inevitably expect to be resolved when such technologies like BCI become increasingly ubiquitous. I will do this in parts II-VII, below. Part II describes the LOAC regime governing commander responsibility. Part III describes brain functions and BCI, BCI's underlying technology, and key issues BCI poses for the LOAC legal regime. Part IV analyzes the intersection of BCI with the LOAC regime. Part V discusses normative implications of the intersection of BCI and

---

[27] *Id.*; *see* Laws and Customs of War on Land art. 23(e), (Oct. 18, 1907), 36 Stat. 2227, 1 Bevans 631 [hereinafter Hague Convention (IV)] ("[It] is especially forbidden [to] employ arms, projectiles, or material calculated to cause unnecessary suffering."); s*ee also* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 259 (July 8, 1996) ("[T]he entire law of armed conflict . . . applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future. . . .").

[28] ANNA ROY, NAT'L STRATEGY FOR ARTIFICIAL INTEL. 72, 88 (Arnab Kumar et al. eds., 2018).

the LOAC regime. Part VI provides recommended concepts to deal with the emergence of BCI and its impact on LOAC. Part VII provides conclusory remarks.

III. GENERAL LOAC REQUIREMENTS FOR COMMANDER'S RESPONSIBILITY.

Within LOAC rests the concept of respondeat superior.[29] Respondeat superior holds commanders and other superiors responsible for their own actions and those of their subordinates when there is a failure of accountability for those subordinates under their control.[30] This concept, tracing its roots to antiquity, provides requisite legal requirements to determine the culpability of commanders through a myriad of complex sets of signed documents and normative and customary behavior.[31] One scholar notes that LOAC provides that commanders may be held criminally liable for acts outside of their own omission if: (1) she orders her troop to commit violations of LOAC; (2) she disregards LOAC violations of which she is aware, or should be aware, or for knowing them and taking no action to punish those involved; (3) she incites violations of LOAC; (4) she fails to control troops from violating LOAC; (5) she permits or acquiesces to violations of LOAC; and, (6) she issues manifestly illegal orders that pass on to subordinate troops which violate LOAC.[32]

Language supporting these avenues for culpability and accountability can be found in codified international law.[33] Article 49 of the Geneva Convention I and Article 50 of Geneva Convention II not only provide for commanders' personal culpability, but also provide an obligation to search and bring to justice those who commit grave breaches of the convention.[34] The parties are also responsible for enacting legislation to effectuate these requirements.[35] Substantively, the

---

29 SOLIS, *supra* note 15, at 417.

30 *Id*.

31 Jeremy Dunnaback, *Command Responsibility: A Small-Unit Leader's Perspective*, 108 NW. U. L. REV. 1385, 1396 (2014) ("[T]he international community seems to have settled on the following: [c]ommanders have a legal duty to prevent any law-of-war violations within their chain of command.").

32 SOLIS, *supra* note 15, at 417; *see also* TALLINN MANUAL 2.0, *supra* note 15, at 397 n. 954–55.

33 *See generally* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE U.S. § 102–103 (AM. L. INST. 1987).

34 Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, art. 49 (Aug. 12, 1949), 75 UNTS 31; Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, art. 50 (Aug. 12, 1949), 75 UNTS 85; Convention for the Protection of Cultural Property in the Event of Armed Conflict, art. 28 (May 14, 1954), 249 U.N.T.S. 358.

35 Convention (III) relative to the Treatment of Prisoners of War, art. 129 (Aug. 12, 1949), 75 UNTS 135; Convention (IV) relative to the Treatment of Prisoners of War, art.

additional protocols to the Geneva Conventions provide guidance.[36] These articles attempt to codify legal requirements found in international legal precedent.[37] Relevant language is found in articles 86 and 87 of Additional Protocol I to the Geneva Convention:

> The fact that a breach of the Conventions or of this Protocol was committed by a subordinate does not absolve his superiors from penal disciplinary responsibility, as the case may be, if they knew, or had information which should have enabled them to conclude in the circumstances at the time, that he was committing or was going to commit such a breach and if they did not take all feasible measures within their power to prevent or repress the breach.[38]

Moreover, commanders have a duty to prevent such acts by those they control, and those who violate Convention prohibitions.[39] Relevant language requires that "commensurate with their level of responsibility, commanders ensure that members of the armed forces under their command are aware of their obligations under the Conventions and this Protocol."[40]

And, that signatories to the Convention:

> [R]equire any commander who is aware that subordinates or other persons under his control are going to commit or have committed a breach of the Conventions or of this Protocol . . . initiate such steps as are necessary to prevent such violations of the Conventions or this Protocol and, where appropriate . . . initiate disciplinary or penal action against violators thereof.[41]

The avenues of culpability and accountability for commanders demonstrated in the language found in codified law at minimum, maintain a level of international consensus provided by the number of signatories to the treaty.[42]

---

146 (Aug. 12, 1949), 75 UNTS 287.

36 Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I), arts. 86(2) & 87 (June 8, 1977), 1125 UNTS 3.

37 *See* SOLIS, *supra* note 15, at 436–37; THE JAG LEGAL CTR. & SCH., *supra* note 18, at v–vi (demonstrating that as of 2020, the Geneva Conventions have been signed by almost every nation, which signifies not only that its standards are codified international law, but also serves as customary international law regardless of whether a country is a signatory or maintains reservations or objections to specific clauses); *Amidst New Challenges, Geneva Conventions Mark 70 Years of 'Limiting Brutality' During War*, U.N. (Aug. 13, 2019), https://news.un.org/en/story/2019/08/1044161.

38 Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I), art. 86 & art. 87.

39 *Id.* at art. 87.

40 *Id.*

41 *Id.*

42 *Id.*

Codified international law is not the only body of international law that covers culpability and accountability. Through signed agreements, promulgation of policy, and case law, customary international law also provides authority for a commander's criminal liability for their actions and actions of their subordinates.[43] "Customary international law is law made over time by widespread and consistent state practice, acting from a sense of legal obligation."[44] Consistent state practice can include diplomatic acts or instructions, public measures, or official policy statements of a state. Acting from a sense of legal obligation can include state actions done not merely for habit or courtesy, this can also be shown through official policy statements or official legal opinions by a state on a matter of international law.[45] These practices morph into rules of international law and include agreements in which more than one country signs.[46] For example, the Rome Statute of the International Criminal Court, signed by over 130 countries, provides a framework and process to hold "persons accountable for the most serious crimes of international concern."[47] By its own provisions, it is supplemental to national criminal jurisdictions, and when coupled with the number of country signatories, adds to the body of customary law.[48] Articles 25 and 28 of the statute respectfully provide that "a person shall be criminally responsible and liable for punishment for a crime within the jurisdiction of the Court if that person . . . [o]rders . . . the commission of such crime which in fact occurs or is attempted[.]"[49]

A military commander or person effectively acting as a military

---

43 RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW THE U.S. §§ 102(1)(a)–(c), (2), 103(1); United States v. Mohammad, 398 F. Supp. 3d 1233, 1242 (USCMCR 2019) ("Sources of international law include . . . 'international agreements, and general principles of law.'") (internal citations omitted).

44 Mohammad, 398 F. Supp. 3d at 1242.

45 RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW THE U.S. § 102 cmts. a, b.

46 Mohammad, 398 F. Supp. 3d at 1241–42 (citing Doe v. Exxon Mobile Corp., 654 F.3d 11, 42 (D.C. Cir. 2011), *vacated on other grounds*, 527 Fed. App'x 7 (D.C. Cir. 2013)).

47 U.N.: Rome Statute of The International Criminal Court, art. 1 (July 17, 1998), 37 I.L.M. 999; Symposium, *Redefining International Criminal Law: New Interpretations and New Solutions: Criminal Law: The Constitutionality of The Rome Statute of The International Criminal Court*, 98 J. CRIM. L. & CRIMINOLOGY 983, 991 ("The Rome Statute reflects the convergence of the common law and civil law systems, varying nation by nation, that constitute the global administration of criminal law.").

48 U.N.: Rome Statute of The International Criminal Court, *supra* note 47, art. 1, art. 10; Symposium, *Redefining International Criminal Law*, *supra* note 47, at 1032 ("Other laws of nations include those atrocity crimes confirmed in customary international law that form the subject matter jurisdiction of the Rome Statute, namely, genocide, crimes against humanity, war crimes, and aggression, although the latter crime is neither defined nor enforceable yet for ICC purposes.").

49 U.N.: Rome Statute of The International Criminal Court, *supra* note 47, art. 25 & art. 28.

> commander shall be criminally responsible for crimes within the jurisdiction of the Court committed by forces under his or her effective command and control, or effective authority and control as the case may be, as a result of his or her failure to exercise control properly over such forces, where: That military commander or person either knew or, owing to the circumstances at the time, should have known that the forces were committing or about to commit such crimes; and that military commander or person failed to take all necessary and reasonable measures within his or her power to prevent or repress their commission or to submit the matter to competent authorities for investigation and prosecution.[50]

Clarifying the relationship of subordinate and superior culpability and accountability, the statutes provides that a "superior" shall be held liable for crimes or attempted crimes committed by those under his or her "effective control" where the superior "knew" or "consciously disregards information which clearly" indicates that their subordinates are committing or are about to commit a crime.[51] However, the superior must have "failed to take all necessary and reasonable measures" within their power to prevent or repress the commission of crimes.[52] Lastly, if all else fails, the superior must submit the matter to competent authorities for investigation and prosecution.[53] From its language, avenues 1 through 6 for culpability and accountability, above, are covered in this article.

Other, more specific, statutes convening war crimes tribunals mimic the Rome Statute, specifically the Statute of the International Criminal Tribunal for Rwanda (ICTR) and the updated Statue of the International Criminal Tribunal for the Former Yugoslavia.[54] Both, identical in substance, provide:

> [Violations] committed by a subordinate does not relieve his or her superior of criminal responsibility if he or she knew or had reason to know that the subordinate was about to commit such acts or had done so and the superior failed to take the necessary and reasonable measures to prevent such acts or to punish them thereof.[55]

These statutes also demonstrate international consensus in holding commanders responsible for actions of their troop. Albeit, here, this consensus takes place in the fashion of customary law with roots in international case

---

50 *Id.* at art. 28(1).
51 *Id.*
52 *Id.* at art. 28(2).
53 *Id.*
54 S.C. Res. 955, art. 6 ¶ 3 (Nov. 8, 1994).
55 *Id.*; U.N. Secretary General, *Report Pursuant to Paragraph 2 of Security Council Resolution 808, Annex (1993),* art. 6 ¶ 3 UN Doc. S/25704 (1993).

precedent.[56]

A review of both codified and customary international law leads to core terms and elements that provide the legal regime for respondeat superior.[57] First, there must be a superior-subordinate relationship between a commander and their troops.[58] Commander, as it is used in these statutes, denotes civilian and military officials who by nature of their position effectively control forces, regardless of size.[59] This usually stems from command responsibility, the authority to issue orders, and the ability to impose disciplinary action if not followed. [60] Second, a commander (or superior) must have knowledge or information that gives them a level of awareness of violations occurring.[61] This could mean actual or constructive knowledge, both forms of knowledge prevent a superior from remaining willfully ignorant or nonchalant about LOAC violations.[62] However, neither constructive knowledge nor negligence will be considered a form of strict liability.[63] Third, a commander (or superior) must fail to take any action to prevent violations from occurring or do nothing after the fact to punish those responsible for the violations.[64] This could cover actions such as conducting an investigation, convening a court-martial, or submitting subordinates to international authorities.[65] These elements are interpreted in varying degrees depending on venue or the specific legal regime involved, but they are adequate to cover the basics of the conversation and cover the six avenues for culpability and accountability.[66] The most important point, however, is that this legal regime always hinges on the actions of a commander, or their lack thereof.

---

56 TALLINN MANUAL 2.0, *supra* note 15, at 397–99 n. 955, 960–61.

57 *See* Yamashita v. Styer, 327 U.S. 1, 26, 37 (1946) (J. Murphy, dissenting). There are many more terms here found in statutes, such as who constitutes "armed forces;" who is a "competent authority" to "submit" matters of LOAC violations; what is a "reasonable" or "feasible" measure to punish those who violate LOAC; what is an adequate "investigation" or "prosecution;" etc.? Many of these terms would no doubt be pulled from other international law sources or case law. For example, "armed forces" could mean those considered combatants under articles 2 and 3 of the Geneva Convention. An adequate investigation or prosecution, for example, would be judged according to the standards of the violator's national laws. There is no doubt that these questions may be resolved by the victor(s) in an armed conflict, but preferably under the standards of justice vice, as Justice Murphy notes in a famous case, "revenge and vindictiveness" freely masquerading as "false legalism."

58 *See* SOLIS, *supra* note 15, at 437.

59 *See id.* at 437; *see also* Greg R. Vetter, *Command Responsibility of Non-Military Superiors in the International Criminal Court*, 25 YALE J. INT'L L. 89, 103–05 (2000).

60 *See* SOLIS, *supra* note 15, at 437.

61 *Id.* at 438.

62 *Id.* at 437–38.

63 *See id.* at 436.

64 *See id.* at 428, 436, 438.

65 *See id.* at 428–29.

66 *See, e.g.*, Evan Wallach & Maxine Marcus, *Command Responsibility*, INT'L L. WAR J., http://lawofwar.org/command_responsibility.htm (last visited May 17, 2021).

Culpability and accountability for commanders and other superiors for their actions and those of their subordinates is presumed to be traced human-to-human.[67] Disruptions occur, however, when the scienter of criminal culpability and accountability no longer rest with a human actor, but instead, is driven by factors and actions of a controlled platform or device, which through its system design and function, resembles human-to-human command and control.[68] The drafters of these avenues to culpability and accountability for commanders may not have foreseen future warfare where human intuitive decisions are replaced by algorithmic decisions or manipulation, possibly breaking the casual link of scienter to positive action or to actions of subordinates.[69] However, this disruption may not totally excuse commanders from their responsibilities under LOAC by using these platforms, and the destructive results remain subject to standards provided by international law.[70]

IV. BCI & DISRUPTION.

To understand how BCI affects the neurological process of decision-making by a commander or other superior, and its relation to intent, knowledge, and voluntary acts, it is integral to understand how the brain works in this capacity. The brain controls the ability to think and uses thinking to generate action by the human body.[71] This is done through a system of nerves that connect to other parts of the body directly or through the spinal cord.[72] This system of nerves produces electronic signals when stimulated by nerve cells through the sharing of information, which allows thought and action—which lies at the heart of BCI technology.[73]

The major parts of the brain effectuating decision-making and action are the Cerebrum, Cerebellum, and the brain stem.[74] The Cerebrum controls reading, thinking, learning, speech, emotions, and planned muscle movements.[75] It also

---

67 *See* Vetter, *supra* note 59, at 92, 115.

68 *See* Buchan & Tsagourias, *supra* note 16, at 670–71.

69 *See id.* at 646–47.

70 Legality of the Threat or Use of Nuclear Weapons, *supra* note 27 ("[T]he entire law of armed conflict . . . applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future. . . .").

71 *How the Brain Works*, JOHNS HOPKINS MED., https://www.hopkinsmedicine.org/neurology_neurosurgery/ centers_clinics/brain_tumor/about-brain-tumors/how-the-brain-works.html (last visited May 17, 2021).

72 *Id.*

73 *See* Gonfalonieri, *supra* note 26.

74 *How the Brain Works*, *supra* note 71.

75 *Id.*

controls vision, hearing and other senses.[76] It is divided into two cerebral halves: left and right, which cover their respective, self-explanatory portions.[77] Each halve has four lobes: frontal—which plays a major part in complex cognitive, emotional, and behavioral functioning through the prefrontal cortex,[78] parietal, temporal and occipital.[79] They collectively control personality, decision-making, reasoning, speech, sense, memory, and smell.[80] The Cerebellum, which resides in the back of the brain, controls balance, coordination, and fine muscle control such as walking. It also functions as a means to control posture and balance.[81] Finally, the Brain Stem—which resides at the bottom of the brain and connects the Cerebrum to the spinal cord—controls bodily functions such as breathing, eye movements, heartbeat, and blood pressure.[82] All of these major parts play a role for purposes of this article's discussion as they are impacted by BCI.[83]

BCI generally encompasses systems that allow a user to externally control or communicate with technology using only the electrical signals and impulses that are produced by the aforementioned sections of the brain.[84] The main process in which this occurs, today, is by way of Electroencephalography (EEG).[85] EEG is the physiological process by which a method of choice records electrical activity generated by the brain via electrodes placed on or in the head, particularly, the parts of the brain discussed above.[86] These EEG signals come from the brain, which are then extracted or captured by signal acquisition, subsequently decoded using an algorithm, and either given a control signal for use of exterior platforms or cursor controls.[87] Advanced methods include the use of artificial intelligence, machine learning, neural networks, and deep machine

---

76 *See id.*

77 *See id.*

78 Christopher Bergland, *The Neuroscience of Making a Decision*, PSYCHOL. TODAY (May 6, 2015), https://www.psychologytoday.com/us/blog/the-athletes-way/201505/the-neuroscience-making-decision.

79 *See How the Brain Works*, *supra* note 71.

80 *See id.*

81 *See id.*

82 *See id.*

83 *See* Johnathan Wolpaw et al., *Brain-Computer Interface Technology: A Review of the First International* Meeting, 8 IEEE TRANSACTIONS ON REHAB. ENG'G 164 (June 2000); *see also* Jo Best, *What is a Brain-Computer Interface? Everything You Need to Know About BCIs, Neural Interfaces and the Future of Mind-Reading Computers*, ZDNET (Nov. 13, 2019), https://www.zdnet.com/article/what-is-bci-everything-you-need-to-know-about-brain-computer-interfaces-and-the-future-of-mind-reading-computers/.

84 Wolpaw et al., *supra* note 83, at 164; *see also* Best, *supra* note 83.

85 Best, *supra* note 83.

86 *See* Wolpaw et al., *supra* note 83, at 165; *see also* Schuller, *supra* note 10, at 379, 386, 388; *see also* Buchan & Tsagourias, *supra* note 16, at 648–50 (discussing the concept known as "humans in the loop").

87 Wolpaw et al., *supra* note 83, at 166.

learning processes for pattern recognition, which assists in the rehabilitation or training of a controlling human or artificial platform.[88] Depending on an organization's goal for the use of BCI, either route of using EEG appears adequate for disruption due to the process of capturing, acquiring, encoding, decoding, and producing a control signal. The crux being that original scienter connected to positive action, or even knowledge itself, could be affected in the process, rendering actions by a user involuntary or unreasonable.[89]

It is important to understand that BCI involvement with applications to military operations are not new.[90] From its advent in the 1970s, research has been conducted to figure out how to create more intimate interaction between humans and computers using "biofeedbacks" or "biocybernetics" to assist in the control of vehicles, weaponry, or other systems.[91] What was theoretical in the 1970s, due to lack of technological maturity, is today quite real due to advancements in robotics, artificial intelligence, machine learning, and the use of large data samples.[92] These advancements not only allow for the efficient external control of platforms due to signals from the brain, but they also allow feedback and modification for better performance (brain stimulation, memory capacity, and durability).[93] This in-turn promotes better lethality, speed, adaptability, and efficiency of weapons systems—a prime concern and goal in strategy for technologically advanced nations and their militaries.[94]

As applied to LOAC, which provides a framework for mitigating the destructive nature of technological advancements of weapons used in war, the technological disruption occurs at the point of decision-making and accountability for subordinate actions.[95] According to rules governing respondeat superior, intuition is not enough to be held responsible for subordinates' actions, nor is intuition, alone, good enough to impart culpability or accountability on any individual.[96] There must be a level of intent or knowledge, based on circumstances, followed by a manifested and voluntary act,

---

88 *See* Josh Merel et al., *Encoder-Decoder Optimization for Brain-Computer Interfaces*, 11 PLOS COMPUTATIONAL BIOLOGY 4 (2015).

89 *See* Stephen Rainey et al., *When Thinking is Doing*: *Responsibility for BCI-Mediated Action*, 11 AJOB NEUROSCIENCE 49 (Feb. 3, 2020); Andreas Kuersten, *Legal Ramifications of Brain-Computer-Interface Technology*, 11 AJOB NEUROSCIENCE 61–63 (Feb. 3, 2020) (citing Open Peer Commentaries).

90 Wolpaw et al., *supra* note 83, at 165.

91 *Id.*

92 *Id.* (discussing the technological changes in the field since the 1970s which had led to the advancements seen today).

93 *Cybernetics*, *supra* note 1.

94 Ali, *supra* note 19, at 4–5.

95 *See* SOLIS, *supra* note 15, at 417.

96 *See id.*

or failure to act, which produces foreseeable results and a failure of accountability.[97]

The process described above may limit the respondeat superior regime due to the underlying technology. For instance, an algorithm is a set of step-by-step instructions to a computer in a language it can understand as code.[98] These algorithms are looped in this way to prevent the need to manually type code for every instance.[99] Many algorithms for complex systems and platforms run millions of lines of code.[100] Accordingly, code requires intelligent, automated decision-making to produce algorithms to solve problems.[101]

The implementation of artificial intelligence solves this issue as a process that mimics human thinking by making rational decisions in a given environment based upon information inputted, observed, and experienced.[102] Moreover, machine learning, and other forms of deep-machine learning, assists artificial intelligence in developing algorithms to solve problems and training on massive pre-programmed data sets that are matched via algorithm through a variety of methods such as adversarial competition, micromanagement, neural network filtering, and other corrective measures.[103] The data fed to this process of machine learning and artificial intelligence decision-making can occur simultaneously.[104] This raises the possibility that algorithms produced to encourage or stimulate better performance of a human actor may be driven and dictated by the machine. The end result is that decisions may no longer be human, instead, the machine is in a supervisory capacity with the ability to impose its will through a form of cerebral manipulation.[105] Through the process of machine learning, better and more efficient algorithms are produced to assist artificial intelligence, even to the point of surpassing human competition and

---

97 *See id.* at 436.

98 MICHAEL KEARNS & AARON ROTH, THE ETHICAL ALGORITHM: THE SCI. OF SOCIALLY AWARE ALGORITHM DESIGN 4 (Oxford Univ. Press ed. 2020) ("[A]n algorithm is nothing more than a very precisely specified series of instructions for performing some concrete task."); DARRELL M. WEST & JOHN R. ALLEN, TURNING POINT: POLICY MAKING IN THE ERA OF A.I. 221 (Brookings Inst. Press ed. 2020) ("[A]lgorithms are a sequence of instructions telling a computer what to do.") (internal quotations and citations omitted).

99 KEARNS & ROTH, *supra* note 98, at 9–10.

100 *See id.* at 9; *see also* Cade Metz, *Google is 2 Billion Lines of Code–and It's All in One Place*, WIRED (Sept. 16, 2015), https://www.wired.com/2015/09/google-2-billion-lines-codeand-one-place/.

101 *See* Metz, *supra* note 100.

102 *See* Capt. Salahudin Ali, *Cybersecurity Support of Insider Threat Operations*, 30 GEO. MASON U. C.R.L.J. 1, 14–17 (2019).

103 *See id.* at 15–17.

104 *See id.*

105 *See id.* (discussing the process of how artificial intelligence uses the imputed data and its own algorithms to continually improve without the need for human intervention).

superiority.[106]

BCI also presents issues of cybersecurity and transparency that may affect the ability to impart culpability and accountability on commanders accountable for their actions and those of their subordinates. Cybersecurity is "considered a service that uses a process of protecting information and information systems by preventing, detecting, and responding to unauthorized access" and uses of the network's resources.[107] Transparency is generally considered the ability to understand why an AI makes decisions or selects certain data to make decisions.[108] AI and ML have been plagued by the inability to understand why they choose certain data, as well as the ability to understand and trace decision-making.[109] The ability to discern action, explain why it occurs, or to forensically diagnose action are all present.[110] Moreover, the ability to exploit vulnerabilities, known and unknown, presents additional complications.[111] Not only will it be difficult to diagnose issues of malfunction, but also the ability to protect a user from exploitation by outside actors whether through data manipulation or outright hacking.[112] Both issues will present difficulties in determining culpability.[113]

If a situation arises where an algorithm replaces and dictates manifest action, or lack thereof, due to its decision that such action is most rational, the legal regime holding commanders accountable for even external platform-subordinates may be called into question.[114] It may be difficult to demonstrate where a commander "knew" or "should have known," where any act was indeed

---

106 WEST & ALLEN, *supra* note 98, at 221, 226 (describing the concept of singularity, "[M]achine-based superintelligence [that is] greater than human intelligence.") (internal citation and brackets omitted); *see* Ali, *supra* note 102, at 15 n. 98 (describing the concept of general intelligence, whereas artificial intelligence develops the ability to pull all available sources of knowledge and experience across multiple domains to develop intuitive thought mimicking humans).

107 Ali, *supra* note 102, at 2 (internal quotation marks omitted) (quoting CHRIS JAIKARAN, CONG. RES. SERV., R45127, CYBERSECURITY: SELECTED ISSUES FOR THE 115TH CONGRESS (2018)).

108 Ron Schmelzer, *Towards A More Transparent AI*, FORBES (May 23, 2020), https://www.forbes.com/sites/cognitiveworld/2020/05/23/towards-a-more-transparent-ai/?sh=3035e0773d93.

109 *Id.*; *see also* WEST & ALLEN, *supra* note 98, at 211 (noting that the same AI can be used "for both beneficial and malicious purposes.").

110 Schmelzer, *supra* note 108.

111 KEARNS & ROTH, *supra* note 98, at 7; WEST & ALLEN, *supra* note 98, at 173.

112 KEARNS & ROTH, *supra* note 98, at 7–8; WEST & ALLEN, *supra* note 98, at 211.

113 ANDREW FEICKERT ET AL., CONG. RESEARCH SERV., R45392, U.S. GROUND FORCES ROBOTICS AND AUTONOMOUS SYS. (RAS) AND ARTIFICIAL INTELLIGENCE: CONSIDERATIONS FOR CONG. 30 (2018).

114 *See* ALEXANDER, *supra* note 7, at 816–22 (describing the theories behind various criminal law structures).

voluntary, or where a known foreseeable act occurred when algorithmic decision-making processes dictates otherwise.[115] Without the ability to discern requisite knowledge or intent, and voluntary action, the LOAC regime of respondeat superior will be seriously challenged.

V. INTERSECTION AND APPLICATION.

The above discussion of BCI and LOAC requirements may impact the avenues of culpability and accountability for commanders.[116] A discussion of BCI's impact is appropriately applied to these six avenues given they are covered by the LOAC regimes discussed thus far.

A. Avenue (1) & (6): a commander is liable for orders she issues that violate LOAC. A commander is liable for manifestly illegal orders she issues to subordinates.

In a general scenario, it is abundantly clear that an unambiguous order from a commander to violate LOAC would render her liable if the order is executed by her subordinates.[117] This conclusion is grounded in international law.[118] She would have satisfied the elements provided above in being a commander, having effective control of troops and, potentially, failing to prevent or mitigate violations.[119] The order will be grounded in a finding based explicitly or by reasonable inference that she made the illegal order.[120] For instance, her battle plans and actions that demonstrate they were executed may be used as evidence of her positive act, serving as the precipice for subordinate action.[121] This must

---

115 S.C. Res. 995 ¶ 6 (detailing the circumstances where commanders will be held liable for another's actions).

116 *See* SOLIS, *supra* note 15, at 426–31.

117 *See id.* at 428; *see also supra* Part II.

118 *See* Prosecutor v. Dragomir Milosevic, No. IT-98-29/1-A, 98–106 (Nov. 12, 2009). The accused was charged with a variety of crimes committed based upon his orders. The trial court found him liable for directly ordering his subordinates to commit violations of international law. The Appeals court, however, quashed charges of direct orders after finding a lack of proof regarding "positive" action that demonstrates he ordered subordinates to commit violations. Essentially, there were other reasonable and plausible explanations. One piece of evidence offered was that the accused ordered his troops to comply with international humanitarian law in conducting operations.

119 *See* SOLIS, *supra* note 15, at 428; *see* TALLINN MANUAL 2.0, *supra* note 15, at 397; *see also* Vetter, *supra* note 59, at 119–20.

120 *Dragomir Milosevic*, No. IT-98-29/1-A at 99–100 ("In principle, this approach [of finding guilt for violations based on inference from circumstantial evidence] is not erroneous as such, given that both *actus reus* and the *mens rea* of ordering can be established through inference from circumstantial evidence, provided that those inferences are the only reasonable ones.").

121 *See, e.g.*, *id.* at 99–100; *see, e.g.*, Prosecutor v. Dragomir Milosevic, No. IT-98-29/1-

be proven beyond a reasonable doubt, however, with no other reasonable interpretation of the commander's requisite intent followed by subordinate action being plausible.[122]

BCI would impact this legal regime through multiple arguments that, on the extreme end, her intentions and plans were stimulated during a planning phase to provide plans that violated LOAC. Recall that BCI can be used to train a user for better performance or stimulate brain activity to provide more rational courses-of-action chosen by artificial intelligence.[123] In such an instance, it may be reasonable to conclude, given BCI's nascent nature, that there are other plausible and reasonable reasons why violations occurred. This may prevent a finding beyond a reasonable doubt that a commander ordered her troop to commit violations of LOAC because it presents levels of ambiguity in the development of her mental state, as well as the connection to acts of her subordinates.[124] Essentially, her acts and intent, even intuitively, are not her own. This would also be true if a BCI platform manipulates brain signals through the conversion phase to pass orders which violate LOAC to her subordinates, thus breaking the causal connection between intent and subsequent action.[125]

If the commander is not responsible in this instance, then who is? Recall that civilians and other superiors (or overseers) are also included in the legal regime as commanders.[126] One could argue that the commander is superior, or the scientist overseeing a BCI platform during this instance is responsible for the LOAC violations.[127] This may be unreasonable as one would also have to prove they possessed the requisite intent and positive action to order a LOAC violation.[128] Other, more reasonable explanations, such as negligence or flawed design in the BCI's data architecture, would prevent culpability for plans in which they did not design coming into fruition by acts of the commander's subordinates.[129]

All parties' culpability and accountability in this example would, potentially,

---

T, 318–19 (Dec. 12, 2007).

122 *Dragomir Milosevic*, No. IT-98-29/1-A at 100.

123 Gonfalonieri, *supra* note 26.

124 *Dragomir Milosevic*, No. IT-98-29/1-A at 100–01.

125 *Id.* at 395; *see* Bathaee, *supra* note 12, at 891, 927; *see also* Rainey et al., *supra* note 89, at 51; Kuersten, *supra* note 89, at 61, 63.

126 *See* SOLIS, *supra* note 15, at 417–18; *see also* TALLINN MANUAL 2.0, *supra* note 15, at 397–99; *see also* Vetter, *supra* note 59, at 103–05.

127 *See* SOLIS, *supra* note 15, at 338–39, nn. 60–61 (stating that civilians are liable for LOAC violations depending on their level of involvement, even when they are not considered a party to a conflict).

128 *See* ALEXANDER, *supra* note 7, at 815, 818, 823; *see also* Bathaee, *supra* note 12, at 890, 891.

129 *See* Ali, *supra* note 102, at 14–17, 22.

depend upon what actions they took after the violations occurred.[130] It is not enough for a violation to be present, but there must be a failure to prevent violations or a failure of accountability after-the-fact.[131] If no action was taken, assuming one could prove all other elements, then perhaps culpability may be more plausible.[132] If so, findings may still be difficult to achieve.[133]

B. Avenue (2) & (5): a commander is liable when she disregards LOAC violations of which she is aware, or should be aware, or for knowing them and taking no action to punish those involved. A commander is liable for actions of subordinates for which she acquiesces.

There are instances where international law holds commanders accountable for failing to act on information that would allow them to responsibly prevent LOAC violations or punish those who commit them.[134] The key to this legal regime is based upon a "dereliction of duty."[135] In this instance, the information must be such that it provided sufficient notice, either constructively or explicitly, that LOAC violations would occur or are occurring.[136] If a commander is deemed to have sufficient notice, or constructively deemed to have sufficient notice, she must take action to hold subordinates accountable that are not insufficient or incongruent compared to the LOAC violations she seeks to address.[137]

What is deemed insufficient or incongruent compared with the LOAC violation at hand is based upon the degree of authority and control the commander has of her subordinates.[138] Indeed, international law requires commanders to have sufficient control and authority of troops and not to remain willfully ignorant of information to prevent a LOAC violation.[139] Recall that respondeat superior is not a negligence regime.[140] Previous international law cases have shown or called into question a commander's culpability where ambiguity exists regarding the information a commander had when LOAC violations occurred, and where a commander did not hold subordinates

---

130 Vetter, *supra* note 59, at 89, 119–20.
131 *See* SOLIS, *supra* note 15, at 432; *see also* Vetter, *supra* note 59, at 89, 100.
132 Vetter, *supra* note 59, at 89, 92–93, 99; *see also* SOLIS, *supra* note 15, at 418 (outlining the commanders implicit liability based on inaction and prevention).
133 *See* Prosecutor v. Dragomir Milosevic, No. IT-98-29/1-T, 55, 104 (Dec. 12, 2007).
134 SOLIS, *supra* note 15, at 428.
135 *See id.* at 432.
136 *See id.* at 429.
137 *See id.*
138 *See id.*
139 U.N.: Rome Statute of The International Criminal Court, *supra* note 47, art. 28(b).
140 *See* SOLIS, *supra* note 15, at 432.

accountable.[141] In the absence of direct evidence or strong explicit evidence that sufficient information existed, culpability may be hard to prove.[142]

To assist in analyzing whether adequate information was available to a commander and their failure to address potential and actual LOAC violations, international law has developed a test for inquiry. This test includes: (1) the number of illegal acts; (2) the type of illegal acts; (3) the scope of illegal acts; (4) the time during which the illegal acts occurred; (5) the number of troops involved; (6) the logistics involved, if any; (7) the geographic location of the acts; (8) the widespread occurrences of the acts; (9) the widespread occurrences of the acts; (10) the tactical tempo of operations; (11) the modus operandi of similar illegal acts; (12) officers and staff involved; and, (13) the location of the commander at the time.[143] The existence of these elements may render the commander culpable for her failure to act on adequate information before or after violations occur.[144] If knowledge is proven, the commander may escape culpability by proving such things as published orders, directives, or rules of engagement that put subordinates on notice of their responsibility to adhere to the LOAC regime.[145] A commander may escape liability if he could not reasonably have known about the criminal intent of a subordinate.[146] If not, actions such as forwarding information for investigation to superiors or prosecution via courts martial may suffice; determining whether these actions are adequate or not is an extremely fact-intensive exercise, and requires a degree of value judgment to ensure accountability of subordinates by the commander is not pretextual or a legal fiction.[147] There is no doubt this may be an ex-post facto judgment, subject to the scrutiny of the commander's superiors or worst—her

---

141 *Yamashita*, 327 U.S. at 35–36 (Murphy, J., dissenting) (questioning the commander's liability for failing to effectively control troops when his resources and measures used to control troops have been taken away from him).

142 *Id.* at 38, 40 (highlighting that an inability to control troops alone does not render one guilty of a war crime in the absence of culpability); *see also* SOLIS, *supra* note 15, at 439 ("In *Delalic*, the ICTY concluded that the 'knew or had reason to know' standard set in Article 7(3) of the [ICTY] Statute must be interpreted as requiring the commander: (i) to have 'actual knowledge, established through direct or circumstantial evidence, that his subordinates were committing or about to commit crimes. . .'").

143 Prosecutor v. Delalic, et al. IT-96-21-T, 386 (Nov. 16, 1998).

144 *Id.* at 122.

145 *See* SOLIS, *supra* note 15, at 432–33.

146 *See id.* at 432 (demonstrating that after the May Lai massacre in the Vietnam War, each defendant had been referred to court-martial for their violations after their violations were discovered by General Westmoreland. Moreover, before the incidents occurred, General Westmoreland had published orders regularly forbidding acts constituting war crimes).

147 S.C. Res. 955, art. 6 ¶ 3, art. 7.

adversaries.[148]

BCI presents another challenge to this already nuanced analysis. This is primarily due to the requirement to prove a level of knowledge existed on behalf of the commander.[149] What may appear to be clear information of a LOAC violation may be impacted by the underlying process of BCI through signal acquisition, conversion, output, and rational decision-making of algorithms produced by machine learning.[150] Clearly, if a BCI platform edits orders, rules of engagement, or "weaponeering" limitations that are passed to subordinates without a commander's knowledge, initial preventative requirements of the commander would not be present.[151] Culpability may switch to those who were charged with ensuring the platform would not take such actions, possibly through its digital design.[152] It may also be the case that the commander's superiors or overseers had a responsibility to stop such actions in real-time as they were occurring.[153] On an extreme end, if the commander—or anyone else for that matter—were presented with false information by the BCI that LOAC violations were not occurring, none would be culpable.[154]

Post-LOAC violation, certain actions could provide an avenue to escape culpability when evidence has become available.[155] An analysis of mitigation efforts such as reconfiguration, restructuring of machine learning and algorithm safeguards, as well as better testing and micromanagement of systems could provide sufficient action to ensure violations are not reoccurring.[156] On the personnel end, criminal prosecution, investigations, and a host of other accountability measures may prove adequate depending on the type of violation.[157] If not, the analysis shifts back to whom had sufficient control of subordinates and their perceived failure to address violations of their subordinates.[158]

C. Avenue (3): A Commander is responsible for LOAC violations in which she

---

148 *See* ALEXANDER, *supra* note 7, at 823.

149 *See* SOLIS, *supra* note 15, at 428.

150 S*ee supra* Part IV.

151 *See* SOLIS, *supra* note 15, at 437 (outlining the knowledge requirement for superior liability for actions taken by subordinates); *see* Wallach & Marcus, *supra* note 66.

152 *See* SOLIS, *supra* note 15, at 441.

153 *See id.* at 440–41.

154 *See id.* at 428–29.

155 *See id.* at 451 (outlining a case where a commander was found not culpable for the actions of his subordinates where evidence demonstrated that the commander lacked any sort of knowledge of his subordinates' crimes).

156 *See id*.

157 *See id.* at 452.

158 *See id.*

incites.

Although not a direct order, a commander may be culpable for actions she takes that amount to LOAC violations through implicit motivation.[159] This is action in the form of criminal recklessness, reasonably foreseeing and encouraging violations that occur in which the commander does not take measures to prevent.[160] This requires knowledge that violations will occur by placing others in a position and instigating a commission of a LOAC violation.[161] This is not to be mistaken with negligence; here, the commander's motivation and instigation serve as crucial factors.[162]

BCI's technical process would make proving this avenue of culpability and accountability extremely difficult.[163] Given that it is based upon brain signals—which could be stimulated to drive action—motivation may not be imparted on a commander.[164] Intuition, which is one aspect of BCI, is not enough for liability.[165] Connecting a positive act to such intuition would have to overcome the argument that a BCI did not serve as the motivating factor, and that subordinate actions were caused by the commander's instigation.[166] Possibly a purposeful failure to follow established user protocols for a BCI or, for overseers and other superiors, designing a platform to drive violations of subordinates may be enough to establish culpability.[167] The level of digital forensics to prove this, however, would be difficult.[168] This avenue of culpability and accountability may be the most difficult avenue to establish liability.

D. Avenue (4): A Commander is liable for violations committed by subordinates she fails to control.

Commanders have a duty to discharge their authority to control subordinates when they have effective control.[169] This is another requirement for commanders to avoid derelictions of duty where they are in a position to prevent

---

159 *See id.* at 429–30 (quoting *Trial of Erich Heyer and Six Others*, "111e Essen Lynching Case," British Military Court (Dec. 1945), I LRTWC 88, 89-90).

160 U.N. War Crim. Comm'n, L. Reps. on Trials of War Criminals 88, 89–90 (1947).

161 *Id.* at 89–90.

162 *Id.* at 90, 92.

163 *See* SOLIS, *supra* note 15, at 436; *see also* Wallach & Marcus, *supra* note 66.

164 *See* SOLIS, *supra* note 15, at 436; *see also* Wallach & Marcus, *supra* note 66.

165 *See* SOLIS, *supra* note 15, at 427–33; *see also* Wallach & Marcus, *supra* note 66.

166 *See* Rainey et al., *supra* note 89, at 49–50, 55; Kuersten, *supra* note 89.

167 NICK BOSTROM, SUPERINTELLIGENCE.: PATHS, DANGER, AND STRATEGIES 158 (Oxford Univ. Press ed. 2014).

168 *See supra* Part III.

169 *See* SOLIS, *supra* note 15, at 430; see also Vetter, *supra* note 59, at 89, 102, 105; Wallach & Marcus, *supra* note 66.

LOAC violations or hold those accountable who commit them.[170] Previous cases demonstrate that this responsibility may be imparted on commanders where sufficient information exists that large-scale violations are occurring, where it would be unreasonable to assume that a commander was not aware of such violations, and failed to exercise their authority to prevent violations or hold those accountable who commit them.[171]

BCI provides complications to this regime. Given the underlying technologies' abilities to manipulate inputs and outputs of information via brain signals, a commander may not be able to cross the threshold of being aware of violations.[172] An argument could still be made that, given the technology and its ability to manipulate information, commanders should have taken measures to ensure their information is accurate in the input and output stage.[173] This may amount to negligence or a low level of recklessness, which is not covered by international legal regimes governing respondeat superior.[174] Once information does become available *ex post facto*, a commander will be judged vis-à-vis their actions to hold her subordinates accountable.[175]

In this avenue, an overseer or other superior supervising the commander may be better positioned for accountability.[176] Their actions also must be more than negligence.[177] Failures in programming, training, failsafe mechanisms, or user instructions would not be enough.[178] But, if these parties were aware of what the technology was doing or were aware of its capability to override a commander's brain signals during its employment, it would make them sufficiently aware that widespread violations were occurring.[179] If allowed, they could be deemed to have failed to control such technology and subordinates or, at minimum, acquiesced to the violations which had occurred.[180]

VI. NORMATIVE ARGUMENTS.

Important aspects of technology and its ability to disrupt industry are the ways it impacts normative behaviors developed by society that govern certain

---

170 *See* SOLIS, *supra* note 15, at 430.
171 *See id.* at 446.
172 *See supra* Part III.
173 *See* SOLIS, *supra* note 15, at 338–39 n. 60–61, 432, 732–51; *see also* Vetter, *supra* note 59, at 124.
174 Buchan & Tsagourias, *supra* note 16, at 661.
175 *Id.* at 649.
176 *See* SOLIS, *supra* note 15, at 429.
177 *See id.* at 436–37; *see also* Vetter, *supra* note 59, at 102–05.
178 *See* SOLIS, *supra* note 15, at 437; *see also* Vetter, *supra* note 59, at 115–16; *see also* BOSTROM, supra note 167, at 155–76.
179 *See* SOLIS, *supra* note 15, at 430.
180 *See id.*

activities. Legal regimes do not address all behaviors, oftentimes they address positive questions regarding human activity.[181] Norms govern societal expectations as to how legal regimes are exercised and how legal authority is managed.[182] Answers to these questions are important because we must decide what type of society we want to live in, considering the emergence of invasive technologies that infringe upon one of the most inherent aspects of what it means to be human: the ability to think freely and make voluntary decisions.[183] If algorithms and machines drive thought and decision making, a legitimate question arises as to whether the definition of "human" in future conflict remains accurate where such algorithms and machines drive a decision to take human life.[184] Legal regimes may not be able to accurately govern such activity if a common understanding of norms is not settled.

At a fundamental level, war is a human endeavor.[185] It is an extension of mankind's political aptitude and nature as a means of exercising real-politik—bundled into nation-states, it is merely a clash of wills to achieve objectives.[186] These objectives are comprised of the collective that makes a nation-state, driven by common attitudes rooted in an understanding for survival, and the need to acquire resources.[187] This understanding is inherent in humans as a part of the evolutionary process, one in which machine and its algorithms, have taken no part.[188] Algorithms and machines are not yet capable of comprehending the shared human experience.[189] Although programmed by humans, the advent of methodologies such as machine learning may allow for an evolutionary leap in technology's ability to resemble something akin to reproducing a shared experience.[190] However, this shared experience would be limited to that of the

---

181 *See* Clifton B. Parker, *Law May Be Ineffective If They Don't Reflect Social Norms, Stanford Scholar Says*, STANFORD REP. (Nov. 24, 2014), https://news.stanford.edu.

182 *See id.*

183 *See* Calvin Kraft & James Giordano, *Integrating Brain Science and Law: Neuroscientific Evidence and Legal Perspectives on Protecting Individual Liberties*, 11 FRONTIERS IN NEUROSCI. 1 (2017).

184 *See* Schuller, *supra* note 10, at 389 ("We must determine whether AWS technology could unlawfully dilute this causal link such that we could no longer say that a human *functionally* decided to kill.").

185 U.S. MARINE CORPS, WARFIGHTING 1–5 (Dep't of the Navy, 2018) ("[W]ar is a human enterprise. . . .").

186 *Id.* at 2–3 ("War is an extension of both policy and politics with the addition of military force.").

187 *See* Bart Klem, *Dealing with Scarcity and Violent Conflict* 1, 37 (Neth. Inst. of Int'l Rel. Clingendael Working Paper No. 24, 2003).

188 *See* Max Tegmark, *The Third Stage Of Life? A.I.*, SCI. FRIDAY (Aug. 25, 2017), https://www.sciencefriday.com/articles/tegmark/.

189 *See id.*

190 *See id.*

digital world.[191]

An understanding as to what drives armed conflict and basic instinct of survival and mitigation efforts afforded to fellow humans will remain in the human domain. Due to our shared experience, conflict seeks a resolution as quickly as possible through another inherent quality found in the humans: empathy.[192] Empathy for ceasing the widespread destruction of armed conflict serves as a motivator to reach an accord in ending conflict.[193] This is shown by the myriad of treaties and diplomatic apparatus that seeks to either prevent conflict or bring it to a close once objectives are realized to the satisfaction of each party involved.[194] Empathy in this context is contrary to the brute logic and rationale used to achieve objectives that are programmed into algorithms.[195] Ending a conflict based on empathy, where there remains the possibility of victory, may be illogical in an algorithmic regime.[196]

Some may argue that this is hyperbolic and that emerging technologies such as BCI merely augment human intelligence and thought, which makes humans more efficient and a cerebrally greater species.[197] But this criticism would fail to capture situations where emerging technology has surpassed its human-creator. Empathy and mitigation in armed conflict are basic concepts.[198] It would be disappointing if the efficiency and ability to augment intelligence LOAC seeks to achieve does not result in a better mitigation of the destructive results that inevitably arise from armed conflict.[199]

VII. RECOMMENDATIONS.

The question remains as to what solutions or concepts can be developed to prevent BCI from negatively impacting culpability and accountability regimes in armed conflict. Below are three recommendations that are in development by industry and academia that call attention to problems associated with BCI and provide solutions.

---

191 Zita Fontaine, *Will Machines Ever Be Capable of Empathy?*, TOWARDS DATA SCI. (Sept. 21, 2019), https://towardsdatascience.com/will-machines-ever-be-capable-of-empathy-d5c929ffc0a4.

192 *See* Tegmark, *supra* note 188.

193 *See id.*

194 *See, e.g.*, THE JAG LEGAL CTR. & SCH., *supra* note 18.

195 Fontaine, *supra* note 191.

196 *Id.*

197 Garry Kasparov, *Intelligent Machines Will Teach Us-Not Replace Us*, WALL STREET J. (May 7, 2018), https://www.wsj.com/articles/intelligent-machines-will-teach-usnot-replace-us-1525704147 ("We're not being replaced by AI. We're being promoted.").

198 Fontaine, *supra* note 191.

199 *See, e.g.*, THE JAG LEGAL CTR. & SCH., *supra* note 18.

A. Cognitive Liberty.

Cognitive liberty is the concept that humans should be entitled to make free and competent decisions with respect to the use of technology that affects their thoughts, and it should only be applied with the consent of the subject using them.[200] Some argue this goes as far as being a basic human right.[201] The advent of technologies that impact the neurological process and manipulate thought has produced a body of academic work that advocates for the idea that thought intrusion should be strictly off-limits.[202] Fear of judgment or punishment for thought is the crux of this concept.[203] Indeed, there is legal tradition in protecting thought itself from use and judgment against an actor without positive action.[204] Thought itself cannot be the avenue by which a person is held accountable for a crime or other forms of liability.[205] The ambiguity of what signals are displayed may produce only a correlation, but in legal regimes where life, liberty, or property may be deprived, based upon judgment of the signals, the tradeoffs of what the technology offers may not be worth the cost.

As we have seen above, LOAC does not find intuition to be a violation itself.[206] To hold commanders accountable, legal regimes must ensure the thoughts and actions of commanders are their own.[207] If not, the failure of maintaining cognitive liberty may present a fundamental defense that neurological interference occurred, thus making it impossible to hold commanders responsible for their failure in preventing and addressing actions imparted on them or their subordinates.

B. Jurisdiction of the Mind.

Jurisdiction of the mind is a step further from cognitive liberty; it advocates

---

200 *See* Marcello Ienca, *Preserving the Right to Cognitive Liberty*, SCIENTIFIC AM. (Aug. 1, 2017), https://www.scientificamerican.com/article/preserving-the-right-to-cognitive-liberty/; Justin Koplow, *Three Thoughts on Privacy in the Coming Era of Brain-Computer Interface*, SMU SCI. & TECH L. REV. BLOG (2020), https://smulawjournals.org/stlr/2020/04/01/three-thoughts-on-privacy-in-the-coming-era-of-brain-computer-interface/.

201 *See* Ienca, *supra* note 200.

202 *See* Kraft & Giordano, *supra* note 183.

203 *See id.* at 3.

204 *See id.* at 2.

205 *See* ALEXANDER, *supra* note 7, at 823; *see also* Bathaee, *supra* note 12, at 890.

206 Wallach & Marcus, *supra* note 66; SOLIS, *supra* note 15, at 418; *see also* Vetter, *supra* note 59, at 92–93 (explaining how a leader might insulate himself from potential violations and criminal culpability).

207 *See* SOLIS, *supra* note 15, at 418; *see also* TALLINN MANUAL 2.0, *supra* note 15, at 396-399 nn. 955, 960–61; *see also* Buchan & Tsagourias, *supra* note 16, at 670.

that the point of decision should remain exclusively that of the thinker.[208] Recall that liability and accountability regimes require both thought and positive action—both must be voluntary.[209] If such positive action does not connect to thought, liability cannot be proven.[210]

Contemporary concerns and principles of cybersecurity are present here. As discussed above, cybersecurity seeks to prevent or mitigate unauthorized access and use of network resources, here, brain signals.[211] Widespread adoption of BCI must ensure that outside actors cannot interfere or dictate action in the same way that AI and ML would do so internally to a BCI system. In other words, addressing the vulnerabilities of a system that outside actors may exploit is an ongoing practice.[212] The potential for neurological penetration in the form of hacking is raised certain degrees in armed conflict, especially with sophisticated state actors with assets that could achieve such feats.[213] Given the presence of a variety of information operations, electromagnetic operations, and cyberspace operations, exploitation of BCI technologies would be a fundamental aspect of tactical doctrine to use against another state to achieve the objective of presenting an adversary as illegitimate due to violations of international law.[214]

To ensure and discern true violations from those which are manipulated, efforts must be made to produce technologies with sound cybersecurity practices that prevent the hacking of the mind.

C. Ethical Algorithms and Digital Architecture.

Algorithms are sets of instructions sent to or embedded within a computer with inputs and outputs.[215] Although inputs and outputs occur through the

---

208 *See* Kraft & Giordano, *supra* note 183 (referencing several Supreme Court cases that reinforce the concept that "citizens should be generally free from intrusion into one's privacy and control of one's thoughts").

209 *See* ALEXANDER, *supra* note 7, at 823; *see also* Bathaee, *supra* note 12, at 891–92 (noting that intent and causation are fundamental doctrines in American law).

210 *See* ALEXANDER, *supra* note 7, at 815; *see also* Bathaee, *supra* note 12, at 892–93 (noting the evidence that is used to determine an individual's thought process behind a given crime).

211 *See* Ali, *supra* note 102, at 17–18.

212 *See* Robin Harris, *Hacking Brain-Computer Interfaces*, ZDNET (Feb. 17, 2020), https://www.zdnet.com/article/hacking-brain-computer-interfaces/ (discussing how individuals can hack a BCI and the dangers it poses).

213 *See* OFF. OF DIR. OF NAT'L INTEL., WORLDWIDE THREAT ASSESSMENT OF THE US INTEL. CMTY. 15–16 (2019).

214 *See* ANDREW FEICKERT ET AL., CONG. RESEARCH SERV., R45392, U.S. GROUND FORCES ROBOTICS AND AUTONOMOUS SYS. (RAS) AND ARTIFICIAL INTELLIGENCE: CONSIDERATIONS FOR CONG. 29 (2018).; *see also* Blythe & Calhoun, *supra* note 24, at 41–42 (noting that competitors weaponize technology to benefit them and further their agendas).

215 KEARNS & ROTH, *supra* note 98, at 4 ("[A]n algorithm is nothing more than a very precisely specified series of instructions for performing some concrete task."); WEST &

acquisition and processing of brain signals, BCI is no different.[216] To ensure legal sufficiency, they must be developed in a way to ensure compliance with international law.[217] For respondeat superior, such technologies must provide a way to discern where thought has been manipulated, and/or where commanders (or overseers and other superiors) can prevent manipulation or identify where it has occurred.[218] This can be achieved through international weapons review, sound auditing, and the ability to program and use BCI in an ethical manner.[219] The weapons review process ensures that technologies such as BCI will not present a situation where the technology cannot be controlled, thus violating international legal regimes.[220] Auditing will allow parties to examine the ambiguity of such technologies, such as artificial and machine learning, to figure out why certain actions were taken from thought to positive action.[221] Sound ethical practice will ensure that reckless programming is prevented and does cross the threshold to criminality.

Regarding digital architecture and the control of artificial intelligence, one scholar notes several ways this can be achieved through methods. Some examples include "Boxing," "Incentives," "Stunting," and "Tripwires."[222] First, Boxing confines a system in such a way that it can only affect the external world through restricted, pre-approved channels.[223] Second, Incentives—allows integration into a wider world through its actions that improve human safety and benefit.[224] Third, Stunting constrains a system's cognitive capabilities or its ability to affect key internal processes.[225] Lastly, Tripwires perform diagnostics on a system with a mechanism to shut it down when dangerous activity is detected.[226] Each of these systems seek to address the looming problem of

---

ALLEN, *supra* note 98, at 221 (defining algorithms as "a sequence of instructions telling a computer what to do").

216 *See supra* Part III.

217 Gary Corn, *Cyber Operations and the Imperfect Art of "Translating" the Law of War to New Technologies*, LIEBER INST., U.S. MIL. ACAD. WEST POINT (Sept. 3, 2020), https://lieber.westpoint.edu/cyber-operations-imperfect-translating-law-war-new/.

218 *See* WEST & ALLEN, *supra* note 98, at 174 (noting the concern that as technology advances, and is used more frequently across the world, there is a growing accountability concern for when undesirable outcomes result from the use of such technology).

219 *See id.* at 183–84, 197 (proposing ways to regulate new and innovate technology, like AI, so that it is a benefit to society rather than a liability).

220 *See id.* at 217 (emphasizing the need for human control over evolving and advanced technology).

221 *Id.* at 183–84.

222 BOSTROM, supra note 167, at 155–76.

223 *Id.* at 155–58

224 *Id.*

225 *Id.*

226 *Id.* (arguing that "endowing a superintelligence with an agent-like structure can be a way of increasing predictability and transparency").

control between agent (BCI system) and principle (human), and the capabilities that a system holds which may overpower or manipulate human operators with its superior intelligence.[227] Each come with its own drawbacks, such as a system manipulating an actor into believing it is under control or augmenting other technologies available to overcome limitations.[228] However, these recommendations offer a technical start to the conversation of limiting the capability of a system to overpower a human operator and dictating decisions that the operator would not have made otherwise by addressing the underlying process in which they make decisions.

VIII. CONCLUSION.

Respondeat superior ensures commanders exercise their authority to prevent violations of LOAC.[229] If they are shown to have a superior-subordinate relationship—effective control of subordinates—and information that allows them to prevent violations or hold those who violate LOAC in which they fail to do so, culpability is imparted on them.[230] BCI disrupts this legal regime, in that the algorithm used by a BCI device may serve as a true superior who dictates action of a commander.[231] It may also impact effective control and the information available to prevent or hold those accountable for LOAC violations.[232] International legal regimes requiring mitigation of the destructive results of conflict may not be adequate to address the emergence of a technology such as BCI.[233]

The shared human experience of survivability and empathy cannot be encapsulated by BCI's technology if limitations are not present.[234] New ideas such as the liberty to keep thoughts private, the ability to maintain control over thought and action, and ethical algorithm design and architecture may present solutions.[235] If not, whether armed conflict remains a human endeavor may be

---

227 *Id.* at 158 (noting which AI system may be the safest option and least likely to corrupt or manipulate the human in control).

228 *Id.* at 156–57.

229 *See* Bathaee, *supra* note 12, at 934 (explaining the doctrine of respondeat superior).

230 Wallach & Marcus, *supra* note 66; *see* SOLIS, *supra* note 15, at 418; Vetter, *supra* note 59, at 92–93.

231 BOSTROM, *supra* note 167, at 155–58 (noting which AI system may be the safest option and least likely to corrupt or manipulate the human in control due to an agency-like structure being implemented).

232 *Id.* at 158 (noting than an "Oracle AI system" may corrupt the human in control).

233 *See* Ali, *supra* note 19, at 42–43 (suggesting certain developments that could defend against advanced technological attacks).

234 *See supra* Part V.

235 *See* Kraft & Giordano, *supra* note 183, at 1–2 (referencing several Supreme Court cases that reinforce the concept that "citizens should be generally free from intrusion into one's privacy and control of one's thoughts").

questionable.[236] The decision remains within the control of humanity as to what path we choose to take in the evolution of technologies such as BCI. The choices made now will undoubtedly affect the way in which accountability is interpreted under international law.

---

236 *See* Ali, *supra* note 19, at 5–6 (noting that developments in technology and cyberwarfare could impact tactical decisions in whether or not to engage in armed conflict because doing so no longer comports with the principle of "proportionality").