MILITARY LAW REVIEW

Volume 228 **Issue 2**

TARGETING MR. ROBOTO: DISTINGUISHING HUMANITY IN BRAIN-COMPUTER INTERFACES

COMMANDER GUY W. EDEN*

The body cannot live without the mind.[1]

I. Introduction

Militaries have long recognized the importance of influencing human perception and decision making in warfare.[2] These activities, categorized as information warfare under current United States (U.S.) military doctrine, aim in part at affecting the cognitive processes within the human

* Judge Advocate General's Corps, United States Navy. Presently assigned as the Staff Judge Advocate for Special Operations Command Central, MacDill Air Force Base, Florida. LL.M., 2019, The Judge Advocate General's School, United States Army, Charlottesville, Virginia. J.D., 2005, University of Pittsburgh School of Law; M.A., 2014, United States Naval War College; B.A., 2002, University of Pittsburgh. Previous assignments include Staff Judge Advocate, Commander, Carrier Strike Group ELEVEN, Naval Station Everett, Washington, 2016-2018; Associate Deputy General Counsel, Department of Defense Office of the General Counsel for Intelligence, Pentagon, Washington, District of Columbia, 2015-2016; Deputy Division Director, Navy Office of the Judge Advocate General – Cyber, Information Operations, and Intelligence Law Division, Pentagon, Washington, District of Columbia, 2014-2015; Professional Development Officer, Region Legal Service Office Southeast, Naval Air Station Jacksonville, Florida, 2012-2014; Deputy Region Staff Judge Advocate, Commander, Navy Region Southeast, Naval Air Station Jacksonville, Florida, 2011-2012; Trial Counsel, Region Legal Service Office Southeast, Naval Station Mayport, Florida, 2010-2011; Staff Judge Advocate, Commander, Naval Special Warfare Group FOUR, Joint Base Little Creek-Fort Story, Virginia Beach, Virginia, 2007-2010; Current Operations Legal Advisor, Multi-National Corps – Iraq, Baghdad, Iraq, March – September 2007; Legal Assistance Attorney, Naval Legal Service Office Mid-Atlantic, Naval Station Norfolk, Virginia, 2005-2007. Member of the bar of Pennsylvania.

[1] THE MATRIX (Warner Brothers 1999).

[2] Conrad Crane, *The United States Needs An Information Warfare Command: A Historical Examination*, WAR ON THE ROCKS (June 14, 2019), https://warontherocks.com/2019/06/the-united-states-needs-an-information-warfare-command-a-historical-examination/.

mind.[3] Yet, activities in information warfare are limited in their ability to have a *direct* effect on the human brain; instead information warfare aims to influence or manipulate the information environment or cyberspace with the goal of having an impact on the human end user.

But consider a situation where the intermediary technology between the influencer and the human consumer allows for direct access to the consumer's brain and cognitive process. Here, information warfare could be conducted directly on the human target. Going a step further, if there was a direct interface between man and machine, would it be possible to do more than simply manipulate information or perception? What if it were possible to cause physical harm, or even kill, through the information environment? One piece of science fiction-feeling technology in existence today that could make this possible is the brain-computer interface (BCI), which enables the human brain to directly interact with a computer or information system.[4]

In his 2014 article on applying international humanitarian law (IHL), otherwise known as the law of armed conflict, to future technology, Eric Jensen notes the importance of anticipating legal stress created by new technology.[5] Jensen then highlights the vital role IHL plays in signaling acceptable state practice in relation to new capabilities and technology. He does this through review of a new weapon's compliance with IHL, both as it is developed and as it is employed during warfare.[6] While such signaling certainly addresses the use of the new technology, it also raises a separate, bedeviling question pertinent to BCI: how do we apply IHL in the other direction to target this technology once it is militarized and attached to a soldier's brain? On its face, the question appears straightforward—a BCI used by an adversary to further military operations during hostilities should be targetable under IHL. But looking deeper, the incredible vulnerability of the human brain demands a more nuanced discussion.

---

[3] JOINT CHIEFS OF STAFF, JOINT PUB. 3-13, INFORMATION OPERATIONS I-1 – I-3 (20 Nov. 2014). *See also* U.S. DEP'T OF ARMY, FIELD MANUAL 100-6, INFORMATION OPERATIONS 2-2 (27 Aug. 1996) This expired Army Field Manual provides a wholistic definition of Information Warfare. This definition fully takes into consideration both the human and technological aspects of Information Operations.

[4] Jerry J. Shih et al., *Brain-Computer Interfaces in Medicine*, 87 MAYO CLINIC PROC. 268, 270-73 (2012), https://www.mayoclinicproceedings.org/article/S0025-6196(12)00123-1/pdf [hereinafter Shih et. al.].

[5] Eric Talbot Jensen, *The Future of the Law of Armed Conflict: Ostriches, Butterflies, and Nanobots*, 35 MICH. J. INT'L L. 253, 256 (2014), https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1061&context=mjil [hereinafter Jensen].

[6] *Id.*

Highlighting part of the targeting challenge presented by BCI, consider the direct connection and interaction it creates between the brain and a computer.[7] A networked computer, what we understand to be part of cyberspace, has been identified as the BCI's greatest vulnerability.[8] Certainly, such vulnerability would be exploited in a military context. Thus, it is natural to consider how the BCI, and by extension the human brain, fits into our understanding of the man-made domain of cyberspace. Further, after peeling back how a BCI is designed, its different variations, and its battlefield functions, we are presented with several variables affecting application of IHL targeting principles in countering the technology.

Therefore, in the spirit of the forward thinking advocated by Jensen, this article anticipates and assesses the challenges of targeting BCI. Several factors, both external to the IHL regime and within IHL itself, apply to this assessment. These include our conception of cyberspace, consideration of whether a BCI-enhanced brain remains a person or becomes an object for purposes of IHL targeting, and arguments for the expansion of weapons treaties or international human rights law (IHRL) to address BCI. The article concludes that despite BCI furthering the convergence of man and machine and philosophical discomfort over the brain's place in cyberspace, current application of IHL to the cyber domain offers the most effective model to handling the challenge of BCI.

To accomplish the analysis, this article first provides a general discussion and overview of some existing BCI technology, potential military applications, and BCI vulnerabilities. Next, it describes concerns raised in the newer academic field of neuroethics over the development of BCI, including suggestions that international law be modified in response to this technology. Addressing these concerns, the article then argues that our current understanding of IHL's application to targeting through cyberspace applies effectively to BCI. This argument is buttressed by an exploration of BCI's place in the current conception of the warfighting domain of cyberspace, focusing on whether the brain remains a biological system or whether its function in a cyber system changes the brain's status

---

[7] Shih et al., *supra* note 4, at 268, 270-73.

[8] *See* CHAIRMAN, JOINT CHIEFS OF STAFF, JOINT PUB. 3-12, CYBERSPACE OPERATIONS I-1 to I-4 (8 Jun. 2018) (discussing the make-up and components of cyberspace). *See also* Marcello Ienca and Pim Haselager, *Hacking The Brain*: *Brain-Computer Interfacing Technology and The Ethics of Neurosecurity*, 18 ETHICS AND INFO. TECH. 117 (Apr. 16, 2016) [hereinafter Ienca and Haselager].

to an object for the purpose of applying IHL targeting principles. Concluding that the best approach is to treat the brain as what it is, a biological portion of human body, allows IHL to apply to targeting BCI without the additional developments in international law advocated by some neuroethicists.

II. Brain-Computer Interface (BCI)

While BCI technology is very real—like many other newer technological breakthroughs—science fiction artists offer insight to the potential, and peril, of the technology as its capability increases and becomes more ubiquitous. For example, consider a world where everyone is equipped with a BCI implanted into their brains that enables access to a pervasive cloud database. This database would be capable of storing recordings of everything that a person sees or hears. In addition, the implant could access and provide unlimited data directly to the brain and be utilized to have a conversation or transact business simply by thinking it. This type of technology forms the background of a recent movie called *Anon*.[9]

While many would see this capability as wonderful, *Anon* provides a glimpse of the dangers this type of technology creates in granting direct access to a person's brain and—by extension—their conscious experience. In the movie, a hacker learns how to manipulate the database and, more importantly, the minds of those who are connected to it. The hacker is able to change what individuals see and hear, at one point causing the protagonist in the film to pull his car into busy traffic after making him perceive the road to be clear. The hacker is also able to manipulate memory—not just in the database, but also what is replayed in people's consciousness. Again, in an effort to harm the protagonist, the hacker accesses the database, erases the good memories of the protagonist's dead son, and then replays the protagonist's memory of the day his son was hit by a car in front of him over and over in the protagonist's mind, causing severe mental anguish. The human mind is manipulated through the BCI to alter temporal and spatial perception, to cause mental suffering, and ultimately to commit murder.[10] Thus the movie raises disturbing questions

[9] ANON (Netflix 2018).
[10] *Id.*

about privacy, the sanctity of the human mind, and malicious use of this technology.

While *Anon* takes place in a distant, cyberpunk future, BCI technology exists today. The technology is nowhere near the point of the seamless, on-demand, bi-directional interface seen in *Anon*, but that has not stopped the Defense Advanced Research Projects Agency (DARPA), academia, and private industry from pursuing this goal.[11] While some of these pursuits simply seek to create the ability for the brain to interface with the internet,[12] many projects have the potential for military application, including remotely controlling military aircraft or robots, mental communication between individuals, and enhanced situational awareness through direct access to data.[13] As this technology is perfected and becomes commonplace, there is little doubt it will be exploited for military advantage.[14]

Against the backdrop of rapidly advancing BCI technology, several moral and ethical questions have been raised in the nascent academic field of neuroethics. Some concerns address the ethical and moral dilemmas faced by researchers and neuroscientists as they develop technology that may have dual-use military application.[15] Other neuroethicists have gone further, offering commentary on the adequacy of international law to address their concerns over BCI and other neuroweapons. Neuroethicists taking this approach have raised two specific concerns: whether the

---

[11] *Six Paths to the Nonsurgical Future of Brain-Machine Interfaces*, DEF. ADVANCED RES. PROJECTS AGENCY (May 20, 2019), https://www.darpa.mil/news-events/2019-05-20; *DARPA and the BRAIN Initiative*, DEF. ADVANCED RES. PROJECTS AGENCY https://www.darpa.mil/program/our-research/darpa-and-the-brain-initiative (last visited Apr. 22, 2020) [hereinafter *DARPA*]; Todd Haselton, *Elon Musk: I'm About To Announce A 'Neuralink' Product That Connects Your Brain To Computers*, CNBC (Sept. 11, 2018), https://www.cnbc.com/2018/09/07/elon-musk-discusses-neurolink-on-joe-rogan-podcast.html.

[12] *Id.*

[13] JONATHAN D. MORENO, MIND WARS: BRAIN SCIENCE AND THE MILITARY IN THE 21ST CENTURY 53-59 (2012) [hereinafter MORENO].

[14] Jensen, *supra* note 5, at 256.

[15] *See* MORENO, *supra* note 13, at 185-205; Marcello Ienca et al., *From Healthcare to Warfare and Reverse: How Should We Regulate Dual-Use Neurotechnology?*, 97 NEURON 269-74 (2018), https://www.cell.com/action/showPdf?pii=S0896-6273%2817%2931140-6 [hereinafter Ienca et. al.]; Tim Requarth, *This Is Your Brain. This Is Your Brain as a Weapon*, FOREIGN POLICY (Sept. 2015), https://foreignpolicy.com/2015/09/14/this-is-your-brain-this-is-your-brain-as-a-weapon-darpa-dual-use-neuroscience/ [hereinafter Requarth]; Charles N. Munyon, *Neuroethics of Non-Primary Brain Computer Interface: Focus on Potential Military Applications*, 12 FRONTIERS IN NEUROSCIENCE 696 (Oct. 2018).

existing IHRL regime is adequate in an age where a brain may be directly accessed through the internet or computer, with some advocating for new rights under IHRL,[16] and whether existing weapons treaties are adequate to limit or prevent states from weaponizing this technology.[17]

If adopted as state practice or formalized in international law, this second line of neuroethical advocacy—which directly relates to the application of international law to this technology—has the potential to limit military use of BCI, thus inviting commentary and response from international legal practitioners. To date, the discussion of how militarized BCI—whether utilized for data access and communication or incorporated into weapon systems—will comply with IHL has been limited.[18] Brain-computer interfaces offer their own, stand-alone advantages to militaries and, from unmanned systems to artificial intelligence, may have complementary functions once incorporated into other future weapons.[19] As BCIs' march towards the battlefield appears inevitable, the time is ripe to begin addressing BCI under the lens of IHL.

A. Brain-Computer Interface Technology Generally

As with any new battlefield innovation, we must first have a basic understanding of the underlying technology prior to considering how IHL applies.[20] First emerging in 1964 when Dr. Grey Walter connected wires to a human brain during surgery,[21] the BCI has made steady advances in conjunction with breakthroughs in neuroscience. The technology has found its primary application within the medical field, but it also harbors

---

[16] Marcello Ienca and Roberto Andorno, *Towards New Human Rights In The Age of Neuroscience and Neurotechnology*, 13 LIFE SCI. SOC'Y. AND POLICY (Apr. 26, 2017), https://lsspjournal.biomedcentral.com/articles/10.1186/s40504-017-0050-1 [hereinafter Ienca and Andorno]; Ellen M. McGee, *Should There Be a Law—Brain Chips: Ethical and Policy Issues*, 24 T. M. COOLEY L. REV. 81 (2007) [hereinafter McGee].

[17] Requarth, *supra* note 15.

[18] Colonel James K. Greer (US Ret.), *Connected Warfare*, MAD SCIENTIST LABORATORY (Jan. 27, 2019), https://madsciblog.tradoc.army.mil/113-connected-warfare/ [hereinafter Greer].

[19] *Id.*

[20] Peter Pascucci, *Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution*, 26 MINN. J. INT'L L. 419, 422 (2017), https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1256&context=mjil.

[21] Alzbeta Krausova, *Legal Aspects of Brain-Computer Interfaces*, 8 MASARYK U. J.L. & TECH. 199, 200 (2014), https://www.researchgate.net/publication/292846508_Legal_aspects_of_brain-computer_interfaces [hereinafter Krausova].

great potential in robotics, prosthetics, and interfacing with information systems.[22] A fully capable brain interface with an information system is a goal being pursued by the U.S. Government, other countries, and private industry; and, there are those that believe such technology is inevitable.[23]

Simplistically, a BCI is a device that enables the brain to directly interact with an external information system or computer through technology implanted into a person's brain or worn externally on a person's skull.[24] A BCI reads the electrical signals in a person's brain associated with different functions, which are then communicated to a computer where the signals are decoded and utilized by that computer to accomplish a task or produce a specific output.[25] The output could be the transfer of information or communication,[26] or it could be utilized to control a mechanism—such as a prosthetic or robotic system.[27] It is important to note that BCI should not be confused with voice or muscle-activated devices—BCI are a mechanism allowing for direct communication between the human brain and computer.[28]

A BCI utilizes a cycle allowing for the brain to input information to the system and later receive feedback.[29] The generation phase of the cycle refers to the brain's creation of electrical signals associated with different tasks or actions.[30] These signals are then read in the second, measurement phase of the cycle, which is facilitated either by an implanted intracranial device or sensors worn externally on the skull.[31] Next is the decoding

---

[22] *Id.* at 200-02.

[23] Adam Piore, *The Surgeon Who Wants to Connect You to the Internet with a Brain Implant*, MIT TECH. REV. (Nov. 30, 2017), https://www.technologyreview.com/s/609232/the-surgeon-who-wants-to-connect-you-to-the-internet-with-a-brain-implant/ [hereinafter Piore].

[24] Shih et al., *supra* note 4, at 268, 270-73.

[25] *Id.*

[26] Linxing Jiang et al., *BrainNet: A Multi-Person Brain-to-Brain Interface for Direct Collaboration Between Brains*, 9 SCIENTIFIC REP. 1 (Apr. 16, 2019), https://www.nature.com/articles/s41598-019-41895-7.pdf.

[27] *Man With Spinal Cord Injury Uses Brain Computer Interface to Move Prosthetic Arm with His Thoughts*, U. OF PITT. MED. CTR. (Oct. 10, 2011), https://www.upmc.com/media/news/BCI-press-release [hereinafter *Brain Computer Interface*]; Patrick Tucker, *It's Now Possible to Telepathically Communicate with a Drone Swarm*, DEFENSE ONE (Sept. 6, 2018), https://www.defenseone.com/technology/2018/09/its-now-possible-telepathically-communicate-drone-swarm/151068/ [hereinafter Tucker].

[28] Shih et al., *supra* note 4, at 268.

[29] Ienca and Haselager, *supra* note 8.

[30] *Id.*

[31] *Id.*

phase, where the measured input from the brain is decoded and classified by a connected computer.[32] Finally, once decoded, the BCI completes the output phase of the cycle.[33] In this phase, the computer executes the brain's intent, whether it be to communicate information or to cause a machine to move.[34] This final phase also provides feedback to the brain on the action.[35]

Neuroscientists are researching both externally worn and implanted devices to facilitate the measurement and output phases of the BCI cycle. Externally worn devices include electroencephalography (EEG) caps which measure the brain's electrical activity through the skull.[36] Internally implanted devices include wired nodes attached directly to the brain[37] and experimental technology like "neural lace."[38] While each allows the BCI cycle to function, internally implanted devices currently have greater capability.[39]

Brain-computer interfaces first saw application in treatment of various medical conditions. Initial iterations were aimed at helping patients who

---

[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] *See* Fiona MacDonald, *Direct Brain-to-Brain Connection Has Been Established Between Humans For The Second Time*, SCIENCE ALERT (Nov. 6, 2014), https://www.sciencealert.com/direct-brain-to-brain-connection-has-been-established-between-humans-for-the-second-time [hereinafter MacDonald] (describing the use of an externally worn EEG cap to facilitate the highlighted research).
[37] Al Emondi, *Neural Engineering System Design (NESD)*, DEF. ADVANCED RES. PROJECTS AGENCY, https://www.darpa.mil/program/neural-engineering-system-design (last visited Apr. 23, 2020) [hereinafter Emondi *NESD*]. This project aims to create an implantable, bi-directional BCI device capable of communicating with one million neurons at a time. This would be a huge step forward for this technology and allow for much greater information flow between the brain and computer system.
[38] Kiki Sanford, *Will This "Neural-Lace" Brain Implant Help Us Compete With AI?*, NAUTILUS (Apr. 4, 2018), http://nautil.us/blog/-will-this-neural-lace-brain-implant-help-us-compete-with-ai; Guosong Hong et al., *Mesh Electronics: A New Paradigm For Tissue-Like Brain Probes*, 50 CURRENT OPINION IN NEUROBIOLOGY 33, 34-36 (2018), http://cml.harvard.edu/assets/Mesh-electronics-a-new-paradigm-for-tissue-like-brain-probes.pdf. Neural-Lace technology is injected by a syringe into the brain, where it unfurls itself and meshes directly with brain tissue. *Id.* By allowing for direct incorporation of interface technology and brain matter, this technology aims to create a much more capable interface with information systems. *Id.*
[39] Al Emondi, *Next-Generation Nonsurgical Neurotechnology*, DEF. ADVANCED RES. PROJECTS AGENCY, https://www.darpa.mil/program/next-generation-nonsurgical-neurotechnology (last visited Apr. 23, 2020) [hereinafter Emondi *Neurotech*].

were "locked-in" paraplegics,[40] then moved to treating patients suffering from epilepsy and Parkinson's disease.[41] These earliest BCI worked in one direction, from the patient's brain to translation by the computer,[42] but the table was set for future innovation.

Brain-computer interfaces have seen application and rapid development in the field of prosthetics. Doctors and neuroscientists have been successful for years in isolating brain patterns associated with movement, enabling the creation of BCI used to control a prosthetic limb.[43] As the technology has been refined, bi-directional communication between a brain and BCI has enabled users to feel sensations, such as heat and texture, on the objects the prosthetic limb touches.[44]

Beyond the BCI allowing for interaction between man and machine, BCI has also begun enabling direct communication between human brains as well as cooperative problem solving.[45] It has also shown success in enabling physical control over the movement of laboratory animals,[46] and has recently demonstrated the ability for one human to physically control the movement of another through thought.[47]

---

[40] Krausova, *supra* note 21, at 200; McGee, *supra* note 16, at 85. "Locked-in" patients are those that are conscious, but unable to move or communicate effectively. *Id.* The BCI enables these patients to communicate utilizing only their thoughts, which are then translated by a computer to produce an output. *Id.*

[41] Piore, *supra* note 23. When utilizing BCI to treat patients suffering from epilepsy or Parkinson's disease, a computer monitors electrical activity in the brain to detect oncoming tremors or seizures. *Id.* Once a tremor or seizure event is detected, the computer acts automatically to send electrical signals through the BCI to the brain to terminate the event. *Id.*

[42] Shih et al., *supra* note 4, at 268-69.

[43] *Id.* at 269, 271-73; *Brain Computer Interface*, *supra* note 27.

[44] *In a First, Pitt-UPMC Team Help Paralyzed Man Feel Again Through a Mind-Controlled Robotic Arm*, U. OF PITT. MED. CTR. (Oct. 13, 2016), https://www.upmc.com/media/news/BCI_scitransl-lms.

[45] Jiang et al., *supra* note 26. Researchers at the University of Washington and Carnegie Mellon University demonstrated the ability to network a group of individual's brains to collaboratively accomplish a task. *Id.* In this case the group worked together to place a game of Tetris. *Id.*

[46] Krausova, *supra* note 21, at 202; Seung-Schik Yoo et al., *Non-Invasive Brain-to-Brain Interface (BBI): Establishing Functional Links Between Two Brains*, 8 PLOS ONE 1-8 (Apr. 3, 2013), https://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0060410&type=printable. Utilizing BCI technology, researchers were able to control the movement of a rat's tail. *Id.*

[47] MacDonald, *supra* note 36; Rajesh P. N. Rao et al., *A Direct Brain-to-Brain Interface in Humans*, PLOS ONE (Nov. 5, 2014), https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0111332 (Neuroscientists were able to create a BCI

The above are but a few highlights of the progress neuroscientists have made in developing BCI technology. Researchers have demonstrated success in electrical interaction with the brain, brain-to-brain communication, collaborative problem solving, and physical control over external systems, animals, and people. Such developments have clear application in military contexts. But, along with military application, BCI carry inherent vulnerabilities in their systems, exposing the human brains to which they are attached.

B. Military Applications

Neuroscience's potential to impact the future of warfighting and national security has been recognized and invested in for years in the United States.[48] While other government entities—such as the intelligence community—have invested in this research, DARPA has led the charge in defense research into BCI.[49] Invested in heavily during the Obama Administration era, DARPA seeks to expand our understanding of technology utilized to interact directly with the brain through the Brain Research through Advancing Innovative Neurotechnologies (BRAIN) Initiative.[50] Several DARPA sub-projects under the umbrella of the BRAIN Initiative aim to further the military integration of this technology by leveraging partnerships with academia. These projects include seeking to expand the capability and data rate for implantable BCI devices,[51] utilizing BCI to control vehicles such as drone swarms,[52] restoring and

system where one individual could cause another individual to move their hand to push a button. The experiment was centered on a game where they were tasked with defending a city from an incoming rocket attack by firing cannons at the incoming rockets. The catch was these individuals could not actually fire the cannon themselves, a separate group within the BCI system equipped with a cap designed to stimulate their brains held their hands over a firing button. Despite this second group being completely unaware that the game was going on and being located in a separate building, when the individuals in the first group sent the signal to fire through the BCI, the second group's hands moved involuntarily and pressed the fire button with a varying success rate.).

[48] *See* MORENO, *supra* note 13.

[49] *Id*.

[50] *DARPA*, *supra* note 11.

[51] Emondi *NESD*, *supra* note 37.

[52] Tucker, *supra* note 27; Emondi *Neurotech*, *supra* note 39 (Partnering with academia, DARPA was able to demonstrate the ability for individuals to control a swarm of drones utilizing an externally worn BCI device. The drones were under the control of the operator, and could provide feedback through the BCI directly back to the operator's brain. The DARPA led and funded Next-Generation Nonsurgical Neurotechnology (N^3) was utilized

enhancing memory,[53] and cooperative intelligence analysis and target selection.[54]

Beyond its stand-alone capabilities, BCI offers complementary capability to developments in artificial intelligence (AI), allowing humans to directly interact with AI systems instead of simply being in or on the loop.[55] Such convergence blurs the line between man and computer, potentially leading to weapons or weapon systems incorporating the unconscious abilities of the brain to maximize the effectiveness and reactiveness of a military system.[56] Such systems could leverage the human brain's superior ability to unconsciously recognize threats, melding them with an AI computer's superior ability to calculate a response.[57] In these weapon systems, the BCI would function by picking up the brain's unconscious recognition of a threat, passing on that information for an automated response from the AI.[58] A conscious human decision would be left out of the equation.[59]

---

in this research. N^3 aims to expand the capability of externally worn BCI so it can be utilized by able bodied individuals to control vehicles or to interact with computers in cyber defense activities.).

[53] Tristan McClure-Begley, *Restoring Active Memory (RAM)*, DEF. ADVANCED RES. PROJECTS AGENCY, https://www.darpa.mil/program/restoring-active-memory (last visited Apr. 23, 2018); Robert E. Hampson et al., *Developing A Hippocampal Neural Prosthetic To Facilitate Human Memory Encoding And Recall*, 15 J. NEURAL ENG. 1-15 (Mar. 28, 2018), http://iopscience.iop.org/article/10.1088/1741-2552/aaaed7/pdf (Through the RAM program, DARPA aims to help service members recover their memories after suffering a traumatic brain injury. The associated RAM-Replay project aims to enhance the training of able bodied service members by "uploading" information directly into their brains via BCI technology.).

[54] Adrian Stoica et al., *Multi-Brain Fusion and Applications to Intelligence Analysis*, PROC. OF SPIE—INT'L SOC. FOR OPTICAL ENG. 8756 (May 29, 2013) [hereinafter Stoica] (Multiple intelligence analysts are linked via EEG enabled BCI and review imagery. The research indicates enhanced performance in identifying intelligence and targeting information from these networked analysts.).

[55] Greer, *supra* note 18. *See also* Elon Musk & Neuralink, *An Integrated Brain-Machine Interface Platform With Thousands Of Channels*, 21 J. MED. INTERNET RES. 1-14 (Oct. 31, 2019), https://www.jmir.org/2019/10/e16194/pdf; Alex Knapp, *Elon Musk Sees His Neuralink Merging Your Brain With A.I.*, FORBES (July 17, 2019), https://www.forbes.com/sites/alexknapp/2019/07/17/elon-musk-sees-his-neuralink-merging-your-brain-with-ai/#23925b9a4b07 [hereinafter Knapp] (One stated goal of Neuralink is to eventually facilitate interaction between humans and Artificial Intelligence).

[56] Gregor Noll, *Weaponising Neurotechnology: International Humanitarian Law and the Loss of Language*, 2 LONDON REV. OF INT'L L. 201, 204, 207-208 (Feb. 2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2464144 [hereinafter Noll].

[57] *Id*. at 204, 207.

[58] *Id*. at 206-07.

[59] *Id*. at 207.

Significant issues still exist in pursuit of this technology; neuroscience strives to fully understand the way the brain communicates—in essence, its code.[60] Until neuroscientists are able to fully understand this code, the type of BCI that will allow for full integration with AI, computers, and information systems will not be possible.[61] Despite this limitation, the quest for ever more capable BCI drives ahead, opening the door to dangerous vulnerabilities to the BCI and human brain alike.

C. Human Danger Created Through BCI

The direct risk to the human brain created by BCI is caused by BCI's vulnerability to manipulation via cyber means.[62] In essence, once integrated with an information system, a BCI becomes just another node in that system. As P.W. Singer warns, new networked technology rarely incorporates security into its design,[63] and BCI is no different in this regard. Evidence already exists that BCI can be subjected to a cyber-effect or manipulation.

The ability to manipulate implantable medical technology through cyberspace has already been identified as a significant vulnerability. For instance, the Tallinn Manual discusses manipulation of a networked pacemaker using cyber means, causing an effect on an individual's heart.[64] As troubling as it is to be able to manipulate an individual's heart, it is equally—if not more—troubling to be able to manipulate a human brain. This risk is real and has already been demonstrated. A recent Kaspersky Labs report on BCI details vulnerabilities in the systems that interact with and control them.[65] The report highlights the ability to interfere with the software used to control the BCI hardware, creating the ability to steal or manipulate memory, and allowing for direct harm to the individual

---

[60] Piore, *supra* note 23.
[61] *Id*.
[62] Ienca and Haselager, *supra* note 8; Requarth, *supra* note 15.
[63] Peter W. Singer, Senior Fellow, New America, Sommerfield Lecture at The Judge Advocate General's Legal Ctr. and Sch. (Nov. 1, 2018).
[64] NATO COOP. CYBER DEFENCE CENTRE OF EXCELLENCE ET. AL., TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 455 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL] (the example in the manual describes manipulation of a pacemaker to cause a series of heart attacks).
[65] *The Memory Market: Preparing For A Future Where Cyberthreats Target Your Past*, KASPERSKY LAB REP. (Oct. 2018), https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/10/29094959/The-Memory-Market-2018_ENG_final.pdf.

equipped with the BCI by manipulating the electrical signals sent to their brains.[66]

Additional concerns over this type of manipulation have been growing, leading to speculation on the dire risks possible through manipulation of BCI through cyberspace.[67] For instance, "brain-hacking" encompasses BCI vulnerabilities at several points in the cycle.[68] Such activity has the potential for third-parties to access the private information in an individual's brain and to wrest control of the system or machine the BCI is interacting with from the user.[69] This activity could potentially lead to physical and psychological harm, as well as the user losing their sense of agency or self-determination of their own life.[70]

Similarly, the concept of "brainjacking," raised in 2016, concerns itself with malicious cyber actors gaining access to implanted BCI and causing effects within the brain.[71] The risks are associated with implanted medical devices, and the authors who coined the term are quick to note that it does not refer to any form of mind-control.[72] What brainjacking does conceptualize, however, is a change in the implant's settings, throwing off the electrical signals sent to the brain.[73] This, in turn, could lead to several adverse effects to the individual, including tissue damage, impairment of motor function, modification of impulse control, emotions, or affect, and induction of pain.[74]

Additional threats to this technology include cyber manipulation of BCI code or hardware at any point in the BCI cycle. For example, should a hacker or other cyber actor gain access to the input portion of the cycle, they may be able to extract sensitive or personal information about that individual.[75] If the other phases of the cycle (measurement, decoding, and

---

[66] *Id*.
[67] Ienca and Haselager, *supra* note 8.
[68] *Id*.
[69] *Id*.
[70] *Id*.
[71] Rich Wordsworth, *Brainjacking: Are Medical Implants The Next Target For Hackers?*, WIRED (Feb. 21, 2017), https://www.wired.co.uk/article/brainjacking-are-medical-implants-the-next-target-of-hackers [hereinafter Wordsworth]; Laurie Pycroft et al., *Brainjacking: Implant Security Issues in Invasive Neuromodulation*, 92 WORLD NEUROSURGERY 454-62 (2016) [hereinafter Pycroft et. al.].
[72] Wordsworth, *supra* note 71.
[73] *Id*.
[74] Pycroft et al., *supra* note 71.
[75] Ienca and Haselager, *supra* note 8.

output) are compromised, more than data is at risk. The intended output or action can be disrupted or terminated, potentially leaving the individual helpless.[76] In the extreme, the BCI cycle can be hijacked, resulting in physical harm to the individual.[77]

These risks highlight several nightmarish, but entirely plausible, scenarios if BCI reaches its full potential. Imagine the ability to manipulate the motor functions of an individual driving a car, causing them to drive off the road. Further, what if the individual is utilizing a BCI to control a weapon system. Could the physical system be hijacked and turned against the individual or their allies? What if there was potential to disrupt the decision making or personalities of individuals in power? Is it possible to send a signal through the internet to a BCI that causes it to damage an individual's brain to the point of permanently disabling or killing them? These are just a few of the possiblities in a future filled with BCI; spawning a nascent ethical discussion concerning the use of this technology and the role the law will have in its regulation.

III. Neuroethics and Proposals for Regulation

The "mind is surely the most salient feature of *Homo sapiens*."[78] It is not surprising then that neuroethicists are alarmed by the prospect of linking man and machine. Most of the neuroethical discussion centers on the moral and ethical dilemmas presented by BCI; but some neuroethicists push further, advocating for modification or expansion of international law protections in response to advances in neurotechnology. The theme across this discussion is the need to protect the brain and—by extension—mind, consciousness, and human agency.

As a relatively new field in academia, neuroethics aims to advance the discussion of the consequences of new neuroscientific breakthroughs.[79] Identifying the issues presented by BCI, some neuroethicists have focused their attention on government funded dual-use neuroscientific research that furthers BCI and other brain technology, intending to inform scientists

---

[76] *Id*.
[77] *Id*.
[78] Ellen M. McGee and Gerald Q. McGuire Jr., *Becoming Borg to Become Immortal: Regulating Brain Implant Technologies*, 16 CAMBRIDGE Q. HEALTHCARE ETHICS 291, 296 (July 2007).
[79] Requarth, *supra* note 15.

that their latest breakthroughs could have military applications.[80] This portion of neuroethics—relating to research and development—bears directly on moral and ethical questions, with the tangential effect of informing development and review of neuroweapons for IHL compliance.[81] While development of IHL compliant neuroweapons will be essential, this branch of neuroethics does not directly address targeting these weapons once they are deemed compliant and make their way to the battlefield.

Others in the field, viewing the incorporation of this technology into everyday life as inevitable, explore the need for additional laws or expansion of our understanding of human rights protections against abuses of this technology.[82] Some have argued for expansion of IHRL in order to address the threats to the brain created by BCI.[83] Others have highlighted the inapplicability of existing treaties, laws, and regulations to neuroweapons.[84]

The primary driver of neuroethicists' concerns regarding BCI is the potential for the technology to be abused; it could be used to physically damage people's brains—for example, to manipulate individual personality, self-determination, and free will.[85] In response, neuroethicists have identified numerous areas that challenge the ethical use of neurotechnology. First and foremost is the concept of informed consent, which deals with whether an individual has adequately been made aware of the risks associated with the technology.[86]

Informed consent takes on a different dimension when discussing the implantation of BCI or other enhancement technology within service members.[87] The question becomes whether a service member actually has

---

[80] MORENO, *supra* note 13, at 185-205; Ienca et. al., *supra* note 15, at 269-74.
[81] *See* Noll, *supra* note 56 (discussing the development of "neuroweapons.").
[82] *See* Ienca and Andorno, *supra* note 16; McGee, *supra* note 16, at 81; Ienca et al., *supra* note 15, at 269-74.
[83] Ienca and Andorno, *supra* note 16.
[84] *See* McGee, *supra* note 16, at 81; Ienca et al., *supra* note 22, at 269-74; Requarth, *supra* note 15.
[85] McGee, *supra* note 16, at; Ienca et al., *supra* note 22, at 269-74.
[86] Ienca and Haselager, *supra* note 8.
[87] Heather A. Harrison Dinniss and Jann K. Kleffner, *Soldier 2.0: Military Human Enhancement and International Law*, 92 INT'L L. STUD. 432, 452-82 (2016), https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1695&context=ils [hereinafter Dinniss and Kleffner].

a choice.[88] Given the advances in BCI technology, and the risks to the mental livelihood of the individual highlighted earlier in this article, individuals equipped with BCI may assume significant risk.[89] Consider further that some of the technology highlighted previously allows for the manipulation of the mental state of individuals, or even physical control over them.[90] It is not unreasonable to consider BCI being utilized to manipulate service members' personalities or instincts to make them more efficient at carrying out their duties. Informed consent, while not a protection from the potential manipulation of this technology, still offers some human agency and decision making to individuals in allowing this technology to be connected to their bodies.

Once connected, neuroethicists warn abuses of BCI can lead to degradation of a person's privacy, the ability to be secure in their thoughts, and their mental and physical safety.[91] Neuroethicists have discussed protection of "[a]utonomy, agency, and personhood."[92] Autonomy and agency are essential aspects of being a human being.[93] Brain-computer interfaces or other technology that can be utilized to restrict or even overcome human autonomy or agency strike at this core.[94] Compromise of autonomy and agency can lead to three major ethical issues: removal of the "intention-action" link resulting in psychological distress, generation of "uncertainty about voluntary character" of the individual equipped with the BCI, and risk to Western jurisprudence which is based in the voluntary control over an individual's own actions.[95] The first two issues are risks to the individual, while the third has societal consequences that may challenge our ability to reach accountability for illegal acts perpetrated by individuals not in control of their own minds or bodies.

It is against this backdrop that neuroethicists have begun suggesting approaches to mitigate against the risks posed by neurotechnology and, specifically, BCI. These approaches include moral and ethical discussions

---

[88] *Id*. at 452-55.
[89] Ienca and Haselager, *supra* note 8.
[90] *Id.*
[91] *Id.* Dinniss and Kleffner, *supra* note 87, at 455-68.
[92] Ienca and Haselager, *supra* note 8.
[93] *Id*.
[94] *Id*.
[95] *Id. See also* Stephen E. White, *Brave New World: Neurowarfare and the Limits of International Humanitarian Law*, 41 CORNELL INT'L L. J. 177, 185-205 (2008), https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1721&context=cilj (discussing how the function of a BCI may hamper our ability to evaluate personal responsibility or criminal liability for violations of IHL).

as well as suggested expansion of international law and regulatory regimes that would govern the development and use of the technology.

A. Ethical and Legal Proposals to Address BCI's Risks

Neuroethicists have begun expanding their discussions into areas of international law, to include IHRL and other regulatory regimes such as weapons treaties. Neurotechnology's impact on IHRL "largely remains a *terra incognita*."[96] Yet, as new neurotechnology—including perfected BCI—becomes more ubiquitous, adaptive developments in IHRL are possible.[97] Failure to recognize the concerns presented by BCI, and the possible expansion of IHRL, has the potential to create a gap in the law where arguments can be made for greater application of IHRL to BCI, regardless of context. Further, adaptation of or additional weapons treaties may restrict otherwise IHL-compliant operations against BCI.

1. Neuroethical Approaches

In concluding his book *Mind Wars*, Dr. Jonathan Moreno advocates a role for advisory boards made up of scientists and ethicists to provide input on the development of new neurological dual use technology.[98] The goal of this committee would not be to stifle development of this technology, but rather to highlight the human risks the technology will create—including potential military applications.[99] The goal of this approach is for neuroscientists and other researchers to be completely aware that their latest breakthrough could also be used for purposes they never thought of or intended.[100]

This approach is one shared by many other neuroethicists. Highlighting the reality that government funded research into neurotechnology will lead to dual use applications, ethicists aim to ensure scientists and researchers operating in this field have been fully informed of the consequences of their work.[101] Going further, others have suggested

---

[96] Ienca and Andorno, *supra* note 16.
[97] *Id.*
[98] MORENO, *supra* note 13, at 196-205.
[99] *Id.*
[100] *Id.*
[101] Requarth, *supra* note 15.

an even more expansive "neurosecurity framework."[102] This framework would consist of three levels: "regulatory intervention, codes of ethical conduct, and awareness-raising activities."[103] The first is a legal consideration and will be discussed later, but the latter two fall into the realm of ethical consideration. The ethical code of conduct would aim to maximize benefit of government- or military-sponsored neuroscientific development while minimizing the risks to individuals and communities.[104] This would include protections like informed consent and the ability to refuse the implantation of neurotechnology without legal repercussions.[105] It would also aim to ensure security measures were incorporated into the technology to provide protection for individuals.[106] The last prong of the neurosecurity framework would take the educational component advocated by Moreno further, to include scientists, researchers, and the public.

2. Advocacy for Legal and Regulatory Expansion

Neuroethicists have also begun openly speaking about expansion of international law and regulatory regimes to protect individuals from the misuse of BCI. These arguments fall under the first prong of the proposed neurosecurity framework discussed above. In spirit, as they highlight many of the horrible possibilities of BCI while noting that the law is inadequate to address these dangers, neuroethical positions reflect the appeal to the "public conscious" found in the Marten's Clause.[107] Although these proposals include both international and domestic regulation, the discussion here will be limited to two areas of neuroethical advocacy in international law: the application of IHRL and existing international weapons treaties to neurotechnology. In advocating their positions, neuroethicists' focus is on the threat to the brain, not the use of neurotechnology such as BCI. Thus, as their positions are reviewed, it is pertinent to ask whether neuroethicists seek to ban the technology or to

---

[102] Ienca et al., *supra* note 15, at 269-74.
[103] *Id.*
[104] *Id.*
[105] *Id.*
[106] *Id.*
[107] Hague Convention IV Respecting the Laws and Customs of War on Land, Oct. 18 1907, 36 Stat. 2227, 1 Bevans 631 (The "Martens Clause" states "Until a more complete code of the laws of war has been issued…the inhabitants and the belligerents remain under the protection and the rule of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity, and the dictates of the public conscious.").

simply outlaw actions or operations that may affect the BCI and—by extension—the brain.

First, in the area of IHRL, many of the neuroethical concerns align with the motivations and protections found in existing customary and IHRL treaty law.[108] However, according to Marcello Ienca and Roberto Andorno, the fit under existing IHRL is not exact.[109] In 2017, they proposed a human rights "normative upgrade" in which they describe, in light of developments in neuroscience, why a series of human rights should be added to existing IHRL.[110] First, and fundamental to Ienca and Andorno, is the right to cognitive liberty.[111] Cognitive liberty is viewed as fundamental and underlying all other mental rights.[112] It includes the right to utilize, or choose not to utilize, neurotechnologies.[113] Cognitive liberty allows for individuals to be free to make "choices about one's own cognitive domain in absence of governmental or non-governmental obstacles, barriers, or prohibitions," to exercise "one's own right to mental integrity," and to have "the possibility of acting in such a way as to take control of one's mental life."[114]

Serving as the foundation for other proposed rights, cognitive liberty supports other additions to IHRL proposed by Ienca and Andorno. These include the rights to mental privacy, mental integrity, and psychological continuity.[115] Mental privacy aims to protect information gleaned from the brain through a BCI.[116] This may include data on an individual from their brain activity to thoughts and memory.[117] Mental integrity references

---

[108] Int'l Covenant on Civil and Political Rights, Dec. 19, 1966, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976) (ICCPR is the closest corollary to the protections advocated by neuroethicists. ICCPR includes the prohibition of torture or cruel, inhuman, or degrading punishment; the prohibition of slavery; and specific rights allowing for "freedom of thought, conscience and religion" as well as "the right to hold opinions without interference. Many of these rights are also viewed as customary international law through *opinio juris*. Current trends in the applicability of ICCPR reflect its application extraterritorially in situations where a state is exercising control over individuals.).

[109] Ienca and Andorno, *supra* note 16.

[110] *Id.*

[111] *Id.* As proposed, "cognitive liberty" as a fundamental human right require all states to recognize the universal application of this right and prevent states from derogating from adhering to its requirements. *Id.*

[112] *Id.*

[113] *Id.*

[114] *Id.*

[115] *Id.*

[116] *Id.*

[117] *Id.*

mental and physical damage that can be created through the compromise of the brain through a BCI.[118] Psychological continuity describes behavioral or psychological changes or issues that may result from misuse of BCI.[119] In closing, Ienca and Andorno argue that these rights should be incorporated into the current IHRL regime or become new IHRL rights.[120]

Beyond IHRL, neuroethicists have also been quick to point out that neuroscience and neurotechnology are not contemplated by existing weapons treaties, specifically the Biological Weapons Convention (BWC) or Chemical Weapons Convention (CWC).[121] Since BCI and other neuroweapons use technology and electronic signaling rather than biologic or chemical means, neuroethicists have noted the BWC and CWC are inapplicable to BCI.[122]

Brain-computer interfaces are also not contemplated under the Convention on Certain Conventional Weapons (CCW).[123] In consideration of the CCW, it is important to note a potential link between BCI and the ongoing discussions regarding a possible sixth additional protocol to the convention relating to Lawful Autonomous Weapon Systems (LAWS).[124] A stated goal of some BCI development projects is to enable direct interaction between a human brain and AI, the centerpiece technology of LAWS.[125] While beyond the scope of this article, if BCI

---

[118] *Id.*
[119] *Id.*
[120] *Id.*
[121] Requarth, *supra* note 15.
[122] *Id. See also* Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, 10 April 1972, 1015 U.N.T.S. 163, 11 I.L.M. 309; Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, 13 January 1993, 1974 U.N.T.S. 45; 32 I.L.M. 800.
[123] Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects (and Protocols) (as amended on 21 Dec. 2001), 10 Oct. 1980, 1342 U.N.T.S. 137 (As its name suggests, this convention is designed to consider and in certain cases prohibit the use of weapons deemed excessively injurious or that are indiscriminate. The convention has seen five additional protocols which either prohibited or clarified the use of certain weapons. Neuroweapons, including BCI, have not been contemplated by the convention, but due to the BWC and CWC being inapplicable to neuroweapons, the CCW would appear to be a superior mechanism for consideration of these types of weapons.).
[124] *See* U.N. Geneva, *Report of the 2019 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems*, ¶ 17, U.N. DOC. CCW/GGE.1/2019/3 (Sept. 25, 2019).
[125] Knapp, *supra* note 55.

technology continues on this trajectory, future consideration of its relationship with LAWS may warrant further exploration.

Regardless, in viewing neuroweapons, to include BCI systems, as items requiring international regulation, some have advocated for expansion of the above treaties to include neuroweapons.[126] Others have noted a new treaty may be necessary.[127] Neuroethicists are clearly not confining their discussion to the moral and ethical issues raised by the technology, but they are openly advocating for expansion of international law to regulate the technology. Such expansion, if it occurs and depending on how it develops, could significantly impact the ability to utilize BCI systems or target them during hostilities. Obviously, if weapons treaties are expanded or a new treaty was agreed upon to ban or limit the use of BCI or weapons used against them, the restriction would be apparent to all signatories. More delicate, however, is the interaction between IHRL and IHL during warfare and how expansion of IHRL could also limit options in targeting BCI.

B. Expanded IHRL for BCI and Its Interaction with IHL

Traditionally, IHRL is the body of law addressing how humans are protected from deprivation of their rights by their *state* and "how the individual might encounter other private actors *within* the State."[128] Therefore, IHRL allows for the "notion that the individual has rights on the international stage" and that international law can regulate how a state and an individual interact.[129] Differing from most international law, "IHRL recognizes rights based on an individual's personhood rather than on one's status as a citizen or subject of a State party to a treaty."[130] IHRL covers a multitude of subject areas, including education, parenting, labor,

---

126 Requarth, *supra* note 15.

127 *Id.*

128 Naz K. Modirzadeh, *Dark Sides of Convergence: A Pro-Civilian Critique of the Extraterritorial Application of Human Rights Law in Armed Conflict*, 86 INT'L L. STUD. SER. U.S. NAVAL WAR COLL. 349, 353 (2010) https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1109&context=ils [hereinafter Modirzadeh].

129 *Id*.

130 INT'L & OPERATIONAL LAW DEP'T, THE JUDGE ADVOCATE GEN.'S LEGAL CTR. & SCH., U.S. ARMY, JA 45, OPERATIONAL LAW HANDBOOK (2018) [hereinafter OPLAW HANDBOOK].

politics, and religion.[131] IHRL's influence on the relationship between an individual and the state is only limited by the scope of how it develops.[132]

IHRL and IHL have been traditionally understood to apply separately of each other.[133] IHRL applies territorially during peacetime, governing the conduct of a state towards its own citizens and individuals under the state's control.[134] IHL applies during wartime, governing the responsibilities states have toward each other in the conduct of hostilities.[135] This position, known as displacement, reflected the long-held international law doctrine of *lex specialis,* which dictates the more specific area of law governs a given situation.[136] Under displacement, IHL is the *lex specialis* governing armed conflict.[137]

However, recent international jurisprudence, opinions of numerous commentators, and burgeoning state practice has shifted the understanding of how IHRL and IHL interact.[138] The current consensus has shifted to a position of convergence where IHRL and IHL apply contemporaneously, even during armed conflict.[139] In this position, IHL would retain its position as the *lex specialis* governing hostilities; but other areas where IHL may not be specific to the situation, or is inadequate to address the question presented, would possibly allow for IHRL's application during armed conflict.[140]

Convergence's mainstream role in the current understanding of how IHRL and IHL interact has raised questions of how to determine when IHRL's application would be triggered during armed conflict.[141] Several authors have noted the impracticality of asking commanders or service members to make a case-by-case determination of which legal regime

---

131 Modirzadeh *supra* note 128, at 353.
132 *Id*.
133 *Id*.
134 *Id*.
135 *Id*.
136 OPLAW HANDBOOK, *supra* note 130, at 51-52.
137 *Id*.
138 WILLIAM H. BOOTHBY, CONFLICT LAW: THE INFLUENCE OF NEW WEAPONS TECHNOLOGY, HUMAN RIGHTS AND EMERGING ACTORS 376-78 (2014) [hereinafter BOOTHBY].
139 *Id*.
140 *Id*.
141 *Id*. *See also* Geoffrey S. Corn, *Mixing Apples and Hand Grenades: The Logical Limit of Applying Human Rights Norms to Armed Conflict*, 1 J. INT'L HUMAN. LEGAL STUD. 52, 90-94 (2010).

applies during a given activity.[142] A more practical suggestion is to divide functions or "broad handfuls" of activities associated with warfare—such as combat operations, logistics, and detention operations—and then make a determination as to which body of law applies to each function.[143] These determinations would apply both in international armed conflict and non-international armed conflict.[144]

Since this article aims to address targeting and engaging BCI, we would appear to be safely in the category of military activities governed by IHL under legal frameworks outlined above. Targeting individuals and military equipment is governed by long established principles for armed conflict under IHL.[145] But BCI offers several other possibilities, such as information operations and intelligence activities, that may not directly implicate IHL's application. Further, some potential capabilities of BCI-enabled weapons, such as a state weaponizing its own citizens or soldiers, have raised questions regarding the applicability of IHL to a state's use of these systems vis-à-vis IHRL.[146] This discussion centers on the applicable law to the creation or use of BCI-enabled weapons by one state, not an adversary's targeting of these weapons or the individuals wielding them.

Care should be taken when considering the arguments of proponents of IHRL or other restrictions on the use of neuroweapons, such as neuroethicists, as to the extent of IHRL's applicability to the problem. A clear articulation of IHL's applicability to targeting BCI, addressing the inherent risks to the human brain highlighted by neuroethicists, is imperative to maintaining the distinction between when IHRL's applicability should end and when IHL's should begin.

IV. BCI, the Brain, and Cyberspace

Before addressing the applicability of IHL to BCI, we must first consider its place on the battlefield. While discussing BCI and other

---

142 BOOTHBY, *supra* note 138, at 376-78.
143 *Id.*
144 *Id.*
145 *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I] (establishing the recognized targeting principles of military necessity, distinction, proportionality, and humanity).
146 *See* Noll, *supra* note 56; Dinniss and Kleffner, *supra* note 87, at 455-79.

neuroweapons, neuroethicists focus on the dangers to the human brain; however, another consistent thread is present in their discussions: the threat is mainly resident in cyberspace. A BCI is part of a networked computer system that happens to incorporate the brain. Further, the brain can function similarly to a computer in a BCI system, raising the question of whether it maintains its status as part of a person or is it now an incorporated object due to its function in the man-made cyber domain. While some recent work has explored this question, this approach may serve to complicate the application of IHL to targeting technology such as BCI. This section explores these questions in the context of the brain's place and status during armed conflict.

A. Cyberspace and the Brain, Briefly

Cyberspace consists of the collection of information nodes (computers, servers, routers, etc.) that allow information systems to communicate with each other.[147] First established as a way for academics to communicate and share research data via computer, the internet has exploded into an indispensable part of human life.[148] Improvements in telecommunications and processing technology has allowed the cyber domain to extend beyond traditional computers and into many other everyday devices.[149] Our phones, cars, watches, televisions, and even our refrigerators can be connected to the internet, becoming part of the ever increasing cyber domain.[150] The ubiquity of objects connected to the internet makes up what has been referred to as the "Internet of Things (IoT)."[151]

Data flows through the internet in accordance with Transmission Control Protocol/Internet Protocol ("TCP/IP"), the common language of cyberspace.[152] As nodes are added, data is able to flow utilizing TCP/IP to an astoundingly diverse group of devices across the entire globe.[153] A

---

147 Pascucci, *supra* note 20, at 423-26.
148 *Id*.
149 *See* Janna Anderson and Lee Rainie, *The Internet of Things Will Thrive By 2025*, PEW RESEARCH CENTER (2014), http://www.pewinternet.org/2014/05/14/internet-of-things/ [hereinafter Anderson and Rainie].
150 *Id*.
151 *Id*.
152 Pascucci, *supra* note 20, at 423-26 (citing Robert Sanchez, *What is TCP/IP and How Does It Make the Internet Work?*, HOSTINGADVICE.COM (Nov. 17, 2015), http://www.hostingadvice.com/blog/tcpip-make-internet-work/).
153 *Id*.

BCI that is attached to a network is designed to utilize this same language, incorporating the technology into IoT.

Traditionally, when discussing cyberspace, a distinction has been made between the natural world and the man-made realm.[154] For example, the Tallinn Manual discusses cyberspace as consisting of three, man-made layers: physical (network components and infrastructure), logical (applications, data, and protocols allowing for connections between devices), and social (individuals and groups engaged in activities within cyberspace).[155] Department of Defense Joint Doctrine contains a similar description of cyberspace, declaring it exists wholly within the information realm and consists of three layers: physical network, logical network, and cyber-persona.[156]

These descriptions confine cyberspace to a man-made construct, and, therefore, a gap exists between humanity and cyberspace. This gap is currently bridged by the typing of our fingers on a keyboard, the information displayed on a screen that is taken in and processed by our brains, or other current technology allowing humans to interact with cyberspace.[157] In each, human agency and conscious decision making result in the use of an input device or consumption of information produced by cyberspace. There is a clear separation between man and machine.

Humanity's desire to have greater access to the internet, and the data it contains, will make BCI an attractive option to many. Individuals are looking for ways to do away with external devices, with many implanting chips into their bodies already.[158] Humans are already able to wear cyber nodes and hold them in the palms of their hands in the form of smart phones, watches, and other devices.[159] The next logical step is to take away the intermediate technology and to link the human body directly to the cyber domain.[160] It is likely that individuals will be willing to allow their brains to become accessible to cyberspace in exchange for the

---

154 *Id*.
155 TALLINN MANUAL, *supra* note 64, at 12.
156 CHAIRMAN, JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-12, CYBERSPACE OPERATIONS I-1 – I-4 (8 June 2018) [hereinafter CJCSP 3-12].
157 Shih et al., *supra* note 4.
158 *See* Anderson and Rainie, *supra* note 149.
159 *Id.*
160 *Id.*

convenience and access to the internet made possible by BCI. This is where individuals could suddenly find themselves as part of the IoT.

This future will consist of single actions to interact with an information system—brain to computer.[161] There will be no need to move muscles, type, move a mouse, or give a voice command because the BCI will interpret your intent directly from your brain and input it into the information system.[162] The information system could also send data directly back to the individual's brain without even having to bother with a computer display or other output device.[163] Additionally, the brain itself can be incorporated into the information system to enhance its performance or computing power.[164] In each instance, the interface is direct and, based on the definitions of cyberspace above, could arguably incorporate the brain into the physical and logical layers of cyberspace.[165]

Such incorporation of the brain as a cyber-node immediately creates difficulty. As cyberspace is currently understood to be entirely man-made,[166] any addition of a biological system would be a dramatic shift. Brain-computer interfaces offer the ability for the brain to act both as a cyber-node and human user; these functions can occur exclusive to each other or simultaneously.[167] At a minimal level, the brain is providing signals unconsciously through the BCI to the computer it is interacting with in order to facilitate the function of the interface.[168] From a purely functional analysis, there are many aspects of the brain's purpose in a BCI system that are associated with data collection and processing, functions that are traditionally considered part of a computer.[169] This line of thinking has led to some speculation on whether BCI, as a human enhancement, objectifies the brain to which it is attached. In a military context, such a transformation could cause the brain to become a means of warfare or weapon— in other words, affecting the application of IHL.

1. Means, Weapon, or Human?

---

161 *Id.*
162 *Id.*
163 Ienca and Haselager, *supra* note 8.
164 *See* Noll, *supra* note 56. *See also* Stoica, *supra* note 54.
165 Shih et al., *supra* note 4, at 268; CJCSP 3-12, *supra* note 156.
166 CJCSP 3-12, *supra* note 156.
167 Ienca and Haselager, *supra* note 8.
168 *Id.*
169 *Id.*

Consideration that the brain could somehow become objectified due to its function in a BCI system is certainly a dramatic shift. This line of thinking is contrary to the humanitarian spirit of IHL[170] and would base the legal analysis of the application of IHL targeting principles as if the brain in a BCI system had become an object. Such a modification would reduce the protections for persons under IHL, in turn supporting the positions of neuroethicists concerned with the human costs surrounding this technology. From a moral and ethical standpoint, this position does not make much sense. But, considering the question through a purely functional standpoint under IHL, analyzing the brain's purpose and function in a BCI system does illuminate instances where it may act as little more than an object. Therefore, consideration of whether a brain could ever become objectified through its function in a BCI system is warranted.

This question revolves around the brain's function in a given BCI system. For purposes of this analysis, BCI can be broken into two categories: those designed to enable information flow to and from the human equipped with BCI, and those designed to be integrated into a physical system. To the first category, the discussion is fairly straightforward. A BCI designed to simply provide information or data to its host, or to store data for later use from its host, is analogous to our understanding of current computer or information systems.[171]

The brain in this first category of systems retains its human agency and intention. The human's intention to access or provide inputs to the information system is the same in current technology, the utility and direct interaction between the brain and information system offered by the BCI is the only distinguishing factor. Similarly, communication with other individuals through a BCI also requires conscious decisions, which would be undertaken non-verbally and facilitated by the BCI technology.[172] Therefore, a brain connected to BCI in this first category, utilized simply for informational and communication purposes, would clearly retain human qualities.

---

[170] U.S. DEP'T OF DEF., DOD LAW OF WAR MANUAL, para. 1.3.4 (Dec. 2016) [hereinafter LAW OF WAR MANUAL].

[171] *See* Shih et al., *supra* note 4; *See also* CJCSP 3-12, *supra* note 156 (allows for a comparison of the functions of BCI to current cyber capability).

[172] MacDonald, *supra* note 36.

The second category of BCI presents a more significant challenge, as these BCI are designed to control physical systems from a distance.[173] The likely incorporation of BCI into future weapon systems will enable direct control and quicker reaction to potential threats.[174] The military advantages of weapon systems that can move and react more quickly and take decisive action are obvious. The pertinent question under IHL becomes how the brain is designed to interact with such a system.

In a recent paper, Gregor Noll analyzes the role of consciousness and human agency in future weapon systems.[175] The clear advantages of such weapon systems are highlighted, including human superiority to machine in unconsciously recognizing a threat and machine superiority in speed of response.[176] Thus, the potential decisive nature of incorporating both into a BCI weapon systems is laid bare in Noll's discussion by incorporating the best capabilities of man and machine into an automated response.[177] But this decisiveness is only achieved through utilization of the unconscious recognition of the threat by the brain.[178] Noll argues that such weapon systems present a pressing issue for IHL, namely that IHL is built on the conscious human judgment of commanders and those employing weapon systems.[179] Noll highlights that the advantage of BCI weapon systems is lost if a conscious human decision is built into the loop, as it adds time to the decision making chain.[180] Thus, he concludes that excluding a conscious human decision from the loop of these systems is incompatible with IHL as it removes human agency and judgment.[181]

Noll highlights several challenges that will occur when evaluating future BCI weapon systems for compliance under IHL. He also, indirectly, raises the question of what becomes of the brain's status in a weapon system like Noll describes. If the brain is simply there to unconsciously enable the weapon system in execution of its automated or pre-programed function, how is the brain any different from a computer?

---

173 *See supra* note 27.
174 Greer, *supra* note 18; Noll, *supra* note 56.
175 Noll, *supra* note 56.
176 *Id.* at 207.
177 *Id.*
178 *Id.*
179 *Id.* at 210-31.
180 *Id.* at 207.
181 *Id.* at 210-31.

Two other recent articles have broached the question of whether the brain in such a BCI could be considered an object. In the first, Heather Dinniss and Jann Kleffner articulate that certain systems, such as prosthetics, could be weapons if they were designed to cause physical harm or damage.[182] The key feature of this argument is the prosthetic weapon being incorporated into the body of an individual, rather than simply being held or being machinery that is operated through physical manipulation by that individual.[183] By extension, this reasoning could apply to the man-made portions of a BCI, especially if the BCI is designed to control a weapon or weapon system. But this analysis stops short of allowing the brain to be considered part of the weapon, instead focusing on the hardware of the prosthetic as the potential weapon.[184]

A complementary article by Rain Livoja and Luke Chircop expands on this analysis, evaluating whether human enhancement technology could cause a warfighter to become a mean, method, or weapon.[185] The article concludes that the BCI equipped individual is not a method of warfare.[186] It does allow for the man-made portions of the BCI system to be considered a mean of warfare, but again does not include the brain.[187] Interestingly, however, when discussing weapons, the authors make a distinction between weapons and weapon systems.[188] Weapons are defined objects designed to cause physical harm or damage, while weapon systems are considered to be all portions of the system allowing for the function of the weapon.[189] The authors conclude with the possibility that a BCI as a whole can be considered a weapon system, leaving the door open for the brain's inclusion as part of the system.[190] This in turn raises the specter that a brain integrated into a weapon system can be treated as an object instead of part of a person.

Although the door is open to considering the brain as part of a weapon system, this line of thought still requires analysis of the brain's role in the weapon system itself. As Noll articulates, the role of the brain can include

---

[182] Dinniss and Kleffner, *supra* note 87, at 438.
[183] *Id.*
[184] *Id.*
[185] Rain Livoja and Luke Chircop, *Are Enhanced Warfighters Weapons, Means, or Methods of Warfare?*, 94 INT'L L. STUD. 161 (2018), https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1723&context=ils.
[186] *Id.* at 183.
[187] *Id.* at 179-80.
[188] *Id.* at 173-80.
[189] *Id.*
[190] *Id.* at 180.

either unconscious incorporation or allow for conscious human intervention and decision making.[191] A BCI weapon system that incorporates conscious human agency would be similar to a human pulling a trigger or pushing a firing button in a different weapon system. It is not logical to consider the brain in such a system to be part of that weapon system or an object.

But consider systems that utilize the brain unconsciously with no human agency involved. There appears to be some tenuous analysis allowing for consideration of the brain as an object in such weapon systems, since the brain would act like a computer or processor. Taking such a position would be a dramatic shift as part of the human body would become objectified due to its function.

Such an analysis is understandable in an era of human enhancement and convergence between man and machine, but is also radical under the traditional place of a person when applying IHL. Even when BCI technology reaches the point of allowing for such capability, taking the approach of assessing the brain's function in a system to determine its status as a person or object for IHL targeting purposes departs from existing norms of simply treating all humans, and their associated parts, as persons.[192] The very basis of IHL is to mitigate human suffering caused by warfare,[193] so any analysis removing an individual's personhood runs contrary to the spirit of IHL.

Persons, whether they are non-combatant civilians or members of an armed force, are clearly different from buildings, vehicles, weapons, and equipment.[194] This difference between people and objects affects the application of the IHL principles of distinction, proportionality, and humanity.[195] Undergoing a functional analysis of a brain in a BCI system to determine whether it is a person or object serves to overcomplicate the matter and is akin to trying to fit a square peg into a round hole. The role of the brain, and conscious human decision making and agency, is a consideration in whether a BCI-enabled weapon system would comply

---

[191] Noll, *supra* note 56, at 205-07.

[192] LAW OF WAR MANUAL, *supra* note 170, para. 2.5.3. (discussing the IHL principle of distinction, the Law of War Manual cites numerous precedents which broadly refer to persons and objects. At no time is there consideration of whether a part of a person could be considered an object for purposes of analysis under the principle of distinction.).

[193] *Id.* para. 1.3.4.

[194] *Id.* para. 2.5.

[195] *Id.*

with IHL during a weapons review process. But, for purposes of targeting, the better approach is to treat the brain—conscious or unconscious—as a part of a person, allowing for consistent application of IHL and its targeting principles.

V. Applying IHL to Targeting BCI in the Cyber Domain

Beginning from a position that always treats the brain as part of a person for targeting purposes allows for a clearer step-by-step analysis of targeting BCI through cyberspace. IHL is understood to apply in cyberspace.[196] Adversaries utilizing BCI to interact with cyberspace, as they would use a computer or other device, may be legally targeted under IHL through cyberspace;[197] but, significant analysis is required prior to undertaking such an operation. The analysis begins with the threshold question of whether the contemplated operation against a BCI meets the definition of an attack. International Humanitarian Law and its targeting principles apply to attacks against BCI, but operations that fall below the threshold of this definition will require separate consideration. Once an operation is deemed to meet the definition of attack, the next portion of the analysis considers what the target actually is in the BCI system. Is it the BCI hardware, the computer or servers the BCI interacts with, the brain of the individual, or any or all the above? Once the scale of expected effects to a BCI are understood, IHL targeting principles can be applied to determine the legality of the operation. Thus, this framework allows for effects on adversary BCI while also offering protections to the brains of individuals incorporated into the BCI.

A. Cyber Attacks and BCI

The Tallinn Manual offers substantial guidance in determining whether an operation against a BCI could be considered an attack for purposes of applying IHL.[198] The Manual defines an attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[199]

---

196 TALLINN MANUAL, *supra* note 64, at 375.
197 *Id.*
198 *Id*. at 415-416. It is important to note the limitations of the Tallinn Manual. While it serves as an important guide in considering cyber operations in the context of international law, containing the collective views of legal experts, it is not a legally binding document.
199 *Id*.

The distinction of whether a cyber operation is deemed to be an attack is violence—which is not required to be kinetic violence—expected to cause the effects listed in the definition.[200] The Manual specifically notes non-violent operations, such as psychological operations or espionage, do not qualify as attacks.[201]

By excepting non-violent operations from its definition of attack, the Tallinn Manual creates a category of potential operations against BCI that do not have associated protections under IHL.[202] Espionage, whether through cyberspace or other means, is certainly an area of concern created by BCI's access to the brain. Neuroethicists highlight these concerns in their discussions of mental privacy.[203] Such concerns are certainly valid, but they are beyond the scope of this paper. Subsequent consideration of legal and regulatory regimes to address espionage activities against BCI is certainly warranted.

The second non-violent category cited by the Tallinn Manual also requires further consideration. The Manual refers to psychological operations as not rising to the level of an attack for the purposes of applying IHL.[204] Psychological operations, also known as Military Information Support Operations in U.S. doctrine, are "operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals."[205] These operations focus on target audiences, including adversaries as well as friendly and neutral populations.[206] Thus psychological operations allow for actions to influence the thoughts of large groups of individuals who may not be participants in hostilities.

---

[200] *Id*.

[201] *Id*. at 415.

[202] *See* Gary D. Brown, *International Law Applies to Cyber Warfare! Now What?*, 46 SW. L. REV. 355 (Apr. 2017), https://www.swlaw.edu/sites/default/files/2017-08/355%20International%20Law%20Applies%20to%20Cyber%20Warfare-Brown.pdf. This article contains an extensive discussion of cyberspace operations that fall below the threshold of an attack or use of force that would trigger the application of IHL, and the challenging legal considerations associated with these operations. Brain-computer interfaces will place an additional legal consideration and complication on top of the already complex legal considerations surrounding these operations. *Id.*

[203] *See supra* pp. 24-25.

[204] TALLINN MANUAL, *supra* note 64, at 415.

[205] CHAIRMAN, JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-13, INFORMATION OPERATIONS II-9 to -10 (20 Nov. 2014) [hereinafter CJCSI 3-13].

[206] *Id.*

Brain-computer interfaces offer a direct avenue to individual minds while conducting psychological operations. Again, this exposure is reflected in the concerns of neuroethicists, who discuss IHRL freedoms of thought, expression, and political independence.[207] While psychological operations contemplated by the Tallinn Manual are not regulated under IHL principles, they are not specifically prohibited under international law and are viewed as a permissible means of warfare.[208] It is also important to note that psychological operations are aimed to influence a population, not control them.[209] Target audiences of psychological operations maintain the ability to digest the information provided to them and to reach their own conclusion, therefore retaining self-determination and agency over their decisions. Again, as BCI will offer a direct path into the thoughts and minds of individuals, revisiting psychological operations enabled by ever more capable BCI may be warranted.

It is important to note, however, that psychological operations discussed in the Tallinn Manual do not include operations that would result in "mental suffering."[210] The Tallinn Manual specifically includes such operations as attacks, requiring the application of IHL targeting principles.[211] Individualized effects manipulating BCI, such as manipulating memory to create mental anguish or affecting the psychology of the individual, could be counted as an attack for purposes of the Tallinn Manual due to the resultant mental suffering.

So, too, would many of the other conceivable operations against BCI, including actions aimed at killing or injuring the individual connected to the BCI, damage to the BCI hardware, or disabling or hijacking the function of the physical system connected to the BCI. These categories focus on effects of destruction, injury, or damage that manifest themselves outside of cyberspace in the natural world. For operations intended to create such effects, IHL would clearly apply.

But one final category of operations, those solely against data, provides an additional layer of difficulty when considering BCI. Per the Tallinn Manual, operations against data are not per se attacks unless such

---

[207] *See supra* pp. 17-26.
[208] LAW OF WAR MANUAL, *supra* note 170, para. 5.26.1.
[209] *See* CJCSI 3-13, *supra* note 205 (discussing the general concepts of MISO, to include its goals to influence a target audience).
[210] TALLINN MANUAL, *supra* note 64, at 417.
[211] *Id.*

operations also affect the functionality of a system or cause other effects tantamount to an attack.[212] State practice has yet to establish positions on the status of data,[213] so a potential gap exists in our understanding of IHL's application to cyber operations against data. Brain-computer interface technology may exacerbate the existence of this gap. Humans equipped with BCI will likely become assimilators of information as the BCI grants a person immediate access to data.[214] However, making this data inaccessible—or corrupting it in some way—may not rise to the level of impairing the function of a BCI, but it will certainly impact a human who is accustomed to this data being readily available. As humans become more accustomed to this data access, depriving individuals' access or corrupting the data could result in the negative mental and psychological effects detailed by neuroethicists.[215] Some have suggested solutions to the status of data in cyber operations, including Peter Pascucci's suggestion of allowing data that offers a "definitive military advantage or demonstrable military purpose to qualify as a military objective."[216] Such an approach would resolve the matter for operations against data accessed and utilized by BCI during armed conflict, but this matter has yet to be settled.

Despite certain cyber operations or activities not fitting under the definition of attack, the vast majority of potential operations against BCI through cyberspace would be considered attacks for purposes of applying IHL. The function of a BCI makes it more likely that a cyber operation against the BCI system would be considered an attack due to the brain's incorporation into the system. The brain's incorporation into the system brings it into closer proximity to the cyber effects created by a given operation, increasing the likelihood that such effects could harm the brain or affect the function of the system the brain is interacting with. Therefore, it may be more likely that cyber operations against BCI are deemed attacks, triggering the application of IHL and the protections found in the IHL targeting principles.

---

[212] *Id.* at 416-18.

[213] Pascucci, *supra* note 20, at 432, 455.

[214] *Old Human vs. New Human*, MAD SCIENTIST LABORATORY, U.S. ARMY TRAINING AND DOCTRINE COMMAND (Jan. 31, 2019), https://madsciblog.tradoc.army.mil/117-old-human-vs-new-human/ (summarizing point of view of several futurists that humans, partly through convergence with technology, including implantable technology like BCI, will become assimilators of information instead of traditional learners).

[215] *See supra* pp. 17-26.

[216] Pascucci, *supra* note 20, at 455.

B. A Framework for Cyber Operations Against BCI

As highlighted by the neuroethicists, neuroscientists, and computer security professionals, BCI contain cyber vulnerabilities that can be exploited in several ways. William Boothby, addressing how cyber weapons can be employed, notes that any given cyber weapon will have "numerous orders or levels of effect and these must all be considered when weapons law advice is being prepared."[217] Boothby goes on to describe four layers of effects that build on each other: effects on the data contained in the node, network, or computer; the impact the data affects or manipulation has on the computer system; how the performance of the computer system affects the object or facility the computer is attached to; and any injury, damage, or destruction suffered by the persons or objects that rely on the facility.[218] The key to Boothby's framework is that the initial effect that the cyber weapon will actually create is on data. The subsequent effects will be consequent of this initial effect and can be tailored to create the desired end state—whether it simply be data manipulation or physical damage. Finally, Boothby states each cyber weapon must be evaluated separate from the framework to see if it will be indiscriminate.[219]

Boothby's framework is well applied to cyber operations against current information nodes in the cyber domain. However, this framework applied to BCI—while still very usable—may require combining the analysis of the third and fourth layers of effects. This is due to the incorporation—or convergence—of the brain into the information node created by the BCI, making the third and fourth layers indistinguishable from each other. Therefore, for consideration of effects on BCI, it may be more useful to simply consider the effects the cyber weapon would have on the data and hardware in a BCI system, and then any effects on the brain.

Such a framework allows for consideration of both the function and employment of the cyber weapon for compliance under IHL. This, in turn, will allow for specific application of the principle of distinction as the weapon is employed—as the effects will either be targeted at the machine portion of the BCI or at the human brain. It will also allow for easier

---

[217] BOOTHBY, *supra* note 138, at 178-80.
[218] *Id.*
[219] *Id.* at 158.

application of the principle of humanity and, in limited cases, the principle of proportionality.

C. Answering Neuroethical Concerns Through the BCI Targeting Framework

The above BCI targeting framework complements our understanding of the BCI cycle and its components, both machine and human. From our earlier discussion of the BCI cycle, we know that the measurement, decoding, and output phases are associated with machine or computer systems, while the generation and feedback portions of the cycle are associated with the brain.[220] Starting here, we can apply the framework adapted from Boothby to the BCI targeting problem by examining the intended effects of a given operation and how achievement of these effects will impact each portion of a BCI system.

The threshold question will be what effect a commander is hoping to achieve. Once understood, the cyber weapon can be designed and narrowly tailored to create an effect in specific BCI, as well as specific portions of that BCI's cycle. New cyber weapons designed and employed against BCI will require analysis of whether the weapon is designed to cause undue suffering or superfluous injury, and whether the weapon is indiscriminate.[221] Once deemed compliant, the weapon can be fielded and utilized by the military forces of a state.[222] When the weapon is utilized, it will also require separate analysis under IHL for adherence to all IHL targeting principles to ensure it is being employed lawfully.[223] Additionally, due to the fleeting nature of code and vulnerabilities in the cyber domain, cyber weapons, including those that could eventually be employed against BCI, may require ad hoc or just-in-time development prior to employment.[224] To provide cyber weapons capabilities in fleeting circumstances, cyber weapons may very well be employed against BCI and simultaneously evaluated for compliance with IHL and lawful employment.[225]

---

[220] Ienca and Haselager, *supra* note 8; *see supra* pp. 8-9.
[221] BOOTHBY, *supra* note 138, at 158.
[222] *Id.* at 176-81.
[223] *Id.*
[224] *Id.*
[225] *Id.*

The requirement to assess a weapon's compliance with IHL provides initial protections to persons under IHL. This would include the brain in the BCI system, as this analysis would prohibit weapons designed to cause undue suffering or superfluous injury from being fielded.[226] Here, the concerns of neuroethicists regarding the physical and psychological effects of attacks on BCI can be incorporated into the analysis of the weapon's design, highlighting the potential dangers of weapons aimed at creating effects in BCI, aiding in the development of more refined and legally compliant weapons.

Further, a particular attribute of cyber weapons is the ability to scale and tailor effects to individual systems.[227] As cyber weapons will be utilized to target BCI, this same ability to tailor weapons and effects will also be possible, satisfying requirements that these weapons not be indiscriminate. Tailoring a cyber weapon for use against a BCI in a way also provides additional distinction from biological and chemical weapons, which neuroethicists point to as comparable to future neuroweapons.[228] Some methods used to employ biological and chemical weapons, such as simply releasing biological or chemical agents into the atmosphere, are unlawful due to their indiscriminate nature.[229] A tailored cyber weapon directed against a lawfully targetable BCI system does not share this indiscriminate quality.

Turning to employment of a cyber weapon against BCI, recall the discussion of the components of the BCI cycle and how each can be associated with a person or object. Effects aimed at the measurement, decoding, and output phases can be assessed as targeting objects for purposes of the IHL principles, where effects aimed at the generation or feedback phases can be considered operations against a person. The BCI

---

[226] *Id.* at 178-79.

[227] *See* BOOTHBY, *supra* note 138, at 179 *citing* Cordula Droege, *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*, 94 INT'L REV. RED CROSS 533 (Jun. 2012). Boothby discusses the ability to limit cyber effects to certain systems, citing the Stuxnet virus as an example. *Id.* While the code of Stuxnet was present on codes around the world, its effects only manifested themselves in the targeted systems in Iran. *Id.* Still, as Cordula Droege notes, Stuxnet highlights the difficulty in preventing the spread of code around the world, even if it is not creating effects on any of the computers infected with the code. *Id.*

[228] Requarth, *supra* note 15.

[229] Jensen, *supra* note 5, at 255-56, *citing* AP I, *supra* note 145, art. 57 (discrimination requires each specific attack, including each weapon system, to be able to differentiate in the attack and only attack intended targets).

targeting framework could then be applied, evaluating each layer of effects—including those on the human brain. The difference in assessing the human effect, whether intended as a direct effect or a collateral result of the operation, would be dictated by what part of the BCI cycle was targeted. This approach has several advantages. First, it will not require a commander to conduct an analysis of the brain's function in a BCI system, adding an additional layer of complication. Second, it allows for clear application of IHL targeting principles to cyber operations against BCI, reinforcing IHL as the lex specialis for military operations during armed conflict and utilizing legal concepts commanders are familiar with. Finally, as the IHL targeting principles incorporate protections for both combatants and non-combatants, application of these principles provide additional mitigation of the concerns raised by neuroethicists in the context of targeting BCI during hostilities.

This final advantage is reinforced by the framework's emphasis on the principle of humanity in operations against BCI. Reviewing the concerns of neuroethicists, all center on the physical and psychological damage that can be done to the human brain by manipulation of BCI. Clearly, the long-term effects of a damaged brain or loss of psychological well-being are horrific. To arbitrarily inflict such injuries would be cruel and would meet the standard of undue suffering or superfluous injury. While the principle of humanity does not guarantee these injuries would not occur, it does aim to require that these types of injuries would only occur in conjunction with a legitimate military operation and use of a weapon in compliance with IHL. This advantage, and the application of the corresponding protections offered by IHL targeting principles, is discussed below.

1. Military Necessity

First formally articulated in the Lieber Code, military necessity has long been recognized as a principle of IHL.[230] Military necessity justifies

[230] *See generally* Headquarters, U.S. War Dep't, Gen. Order No. 100 art. 14 (Apr. 24, 1863 ("Military necessity, as understood by modern civilized nations, consists in the necessity of those measures which are indispensable for securing the ends of the war, and which are lawful according to the modern law and usages of war."); *see* Hague Convention, *supra*

the use of all measures necessary, not otherwise prohibited by IHL, to bring about the defeat of an enemy.[231] This would include the use of cyber operations or attacks against adversaries equipped with BCI. Such operations would have to be linked to a military requirement, benefit, or objective in order to comply with this principle. This requirement applies to any planned operations against BCI, encompassing both attacks and non-attacks such as psychological operations.[232] During armed conflict, linking operations to military requirements, benefits, or objectives serves as additional mitigation of the concerns raised by neuroscientists. Many of these concerns pertain to hackers violating mental privacy by stealing information from BCI-equipped individuals, cyber actors hijacking the function of BCI, or effects resulting in harm to individuals. Military necessity would allow for these types of effects to take place during armed conflict, but not in an arbitrary manner. A commander intending to conduct such an operation would have to define their purpose or objective, adding a layer of consideration and protection for individuals equipped with BCI. While not an absolute prohibition, military necessity would require an IHL-compliant justification for all contemplated cyber operations against BCI.

2. Distinction

Distinction is a bedrock principle in IHL, providing additional protection to civilians during hostilities by requiring that attacks only be directed at combatant persons or military objects.[233] Distinguishing between a combatant and non-combatant person is different from distinguishing between military and civilian objects, facilities, or equipment.[234] Generally, when applying the IHL principle of distinction

---

note 107; Burrus M. Carnahan, *Lincoln, Lieber and the Laws of War: The Origins and Limits of the Principle of Military Necessity*, 92 AM. J. INT'L. L. 213 (Apr. 1998).

[231] LAW OF WAR MANUAL, *supra* note 170, para. 2.2.

[232] *Id.* para. 2.2.1.

[233] AP I, *supra* note 145, art. 48 ("In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."); Yoram Dinstein, *The Principle of Cyber War in International Armed Conflicts*, 17 J. CONFLICT & SECURITY L. 261 (2012), https://academic.oup.com/jcsl/article/17/2/261/852776#14763768.

[234] AP I, *supra* note 145 art. 48. This document specifically articulates different requirements to distinguish between persons and objects. These differences are re-

to people, the status of the individual's affiliation with an armed service or group is the primary consideration, with consideration of conduct reserved for determining whether a civilian is directly participating in hostilities.[235] Objects, however, are examined under a separate test, evaluating whether they make an effective contribution to military action based on their nature, use, location, or purpose, and then considering the military advantage of destroying, capturing, or neutralizing the object.[236] Additionally, dual use objects, utilized for both military and civilian purposes, are also targetable.[237]

Recall the earlier discussion of the brain's status in a BCI, and the conclusion that the brain should always be treated as a person.[238] This conclusion allows for a clearer analysis of the distinction principle. Effects directed at the measurement, decoding, and output phases of BCI cycle, which are part of the computer or machine portions of the BCI cycle, would be analyzed under the object test for distinction detailed above, while effects directed at the generation and feedback portions of the cycle involving the brain would be analyzed under the person test. Brain-computer interfaces incorporated into adversary military means or weapon systems would be distinguishable as military objects, and the brains connected to, interacting with, and operating these BCI would be distinguishable as combatants, making both targetable. But consider a situation where a civilian BCI is being utilized to carry out an operation, with the civilian unaware that it is taking place or not in control of the activity. This scenario is similar in nature to one involving potential future abilities to tailor biological weapons outlined by Eric Jensen.[239] In that scenario, an unwitting carrier of a biological weapon, known to have

---

enforced by the separate requirements found in Articles 50-56. LAW OF WAR MANUAL, *supra* note 170, para. 2.5.

[235] AP I, *supra* note 145, art. 50 (refers to the definition of combatants found in Article 43 of Protocol I and in Article 4 of the Third Geneva Convention). Article 51(1) and 51(2) re-articulate that the civilian population shall not be the object of attack. *Id.* art. 51.

[236] *See* AP I, *supra* note 145, art. 52; Pascucci, *supra* note 20, at 433-39 (Pascucci notes the application of the object test for distinction is not always straight forward. Particularly in analyzing whether a system's nature, location, use, or purpose contributes to military action, Pascucci highlights civilian systems also utilized for military communication and civilian social media being used for a purpose it was not designed for during armed conflict. By extension, care must be taken to assess each BCI system carefully under the distinction of military objects standard.).

[237] *See* Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, 25 STAN. L. & POL'Y REV. 269, 298 (2014), https://law.stanford.edu/wp-content/uploads/2018/03/schmitt.pdf.

[238] *See supra* pp. 30-39.

[239] Jensen, *supra* note 5, at 254-55.

access to the eventual target of the pathogen, is infected.[240] The biological weapon is genetically engineered to only affect the target of the attack.[241] The pathogen in the person's system is clearly a weapon and is being utilized to carry out an attack, but the individual carrying the weapon has no idea the weapon is even in their system and, due to the narrow tailoring of the weapon, it has no effect on the individual.[242] This scenario creates significant issues under IHL,[243] including how to treat the unwitting carrier of the weapon. A similar type of latent attack is envisioned in a cyber context in the novel *Ghost Fleet*.[244]

Here, a Chinese government hacker gains access to multiple digital devices owned by civilians in the United States, to include government contractors, to move portions of malicious code into the Defense Intelligence Agency for the purpose of collecting intelligence.[245] While this is not an example of an attack as defined by the Tallinn Manual, since it is a cyber espionage activity,[246] it does highlight the possibility to utilize devices carried by human beings to carry malicious code. Ubiquitous BCI utilized by the public would be the ultimate human-portable technological device. A pervasive BCI technology, such as neural lace,[247] would make it impossible to discount that adversaries would take advantage of its vulnerabilities. Adversaries could embed malicious code on these devices without the individual's awareness, using these individuals to carry the malicious code or cyber attack payload to its target in a combination of the scenarios outlined above. In this particular scenario, care would be required to distinguish between the status of the malicious code riding on the hijacked BCI, the BCI hardware, and the connected brain when undertaking an operation to counter the attack. Distinguishing the human whose BCI had been hijacked as a civilian invokes the protections of the separate IHL principle of proportionality.

3. Proportionality

---

240 *Id.*
241 *Id.*
242 *Id.*
243 *Id.* at 312.
244 P. W. SINGER & AUGUST COLE, GHOST FLEET: A NOVEL OF THE NEXT WORLD WAR 37-42 (2015).
245 *Id.*
246 *See supra* pp. 41.
247 *See supra* pp. 10.

The principle of proportionality prohibits "an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[248] Thus, proportionality requires an attacker to first consider two specific factors related to incidental harm to civilians: causation and foreseeability.[249] Causation relates to whether the expected incidental harm would be caused by the attack.[250] Unlike the requirement that the anticipated military advantage be directly related to the attack, there is no corresponding requirement under causation for incidental harm to civilians or civilian objects.[251] Incidental harm can be caused either as a direct result of an attack or "as a result of a series of steps."[252] Foreseeability considers whether incidental harm to civilians or civilian objects could have been expected as the attack was planned or launched.[253] When applying foreseeability in assessing a potential attack, the legal standard is one of reasonableness.[254] In other words, "what should have been foreseen" based on the information on hand, or that could be reasonably expected to be on hand.[255] Once an attacker determines incidental harm is foreseeable, they must then also consider the likelihood such harm would occur.[256] The likelihood of whether incidental harm will occur assists the attacker in considering the weight to place on the incidental harm in the larger proportionality analysis. After causation and foreseeability have been fully considered, to complete the proportionality analysis, these considerations must be weighed against the anticipated military advantage to be gained by the attack.[257] "[P]roportionality prohibits attacks expected to cause incidental harm that would be 'excessive' in relation to the anticipated concrete and direct military advantage."[258]

---

[248] AP I, *supra* note 145, art. 51.

[249] Emanuela-Chiara Gillard, *Proportionality in the Conduct of Hostilities: The Incidental Harm Side of the Assessment*, CHATHAM HOUSE 13-20 (Dec. 2018), https://www.chathamhouse.org/sites/default/files/publications/research/2018-12-10-proportionality-conduct-hostilities-incidental-harm-gillard-final.pdf [hereinafter Gillard].

[250] *Id*. at 13-15.

[251] *Id*. at 14.

[252] *Id.* at 18-20; *See also* Pascucci *supra* note 20, at 449-51. Both documents discuss reverberating or "knock-on" effects when applying the principle of proportionality. Specifically, reverberating effects are not directly caused by the attack, but rather are follow on, indirect consequences. *Id.*

[253] Gillard, *supra* note 249, at 15-17.

[254] *Id.* at 16-17.

[255] *Id.*

[256] *Id.* at 16-18.

[257] *Id.* at 20-25.

[258] *Id.* at 21.

Proportionality would initially appear to provide little difficulty in application to BCI. Operations against BCI distinguished as military objects connected to brains belonging to adversaries could be tailored to limit effects solely to these military targets, essentially making proportionality moot. Further, operations exclusively against military BCI hardware would also seem to leave civilian or collateral effects out of the calculus. But, as detailed in the discussion of distinction, scenarios such as brain-hacking, brainjacking, or involuntary manipulation of civilian BCI could lead to otherwise-civilian BCI hardware being utilized for military purposes.[259] Defending against this threat may require disabling the BCI implanted within the individual or interfering with its functionality—either temporarily or permanently. These effects could create detrimental psychological effects in these civilians envisioned by neuroethicists.[260]

Such a scenario adds to the difficulty in applying the principle of proportionality in cyberspace. While the Tallinn Manual allows that effects resulting in mental suffering can be considered attacks,[261] the suffering in this scenario would be a collateral effect on a civilian brain caused by taking action against malicious code within their BCI. But what manipulation or effect in the hijacked BCI would be required to counter the malicious code? Following the above framework for operations against BCI, the hijacked BCI could be considered a military target as a dual-use object. But, as Peter Pascucci highlights and per the Tallinn Manual operations, that would affect the functionality of the BCI and would be considered attacks; however, open questions remain as to whether simply manipulating data would rise to this standard.[262] This creates a potential scenario where data is manipulated in a civilian's BCI hardware to a level not meeting a clear standard of attack, yet still causing a collateral effect of mental suffering in a civilian brain connected to a BCI.

---

[259] *See supra* pp. 14-17.

[260] Ienca and Andorno, *supra* note 16 (discussing the proposed new human rights of mental integrity and psychological continuity, the authors detail how manipulation of a BCI could damage their neural computational and functional abilities, as well as affect their psychological well-being through consequent behavioral changes or perception of the world around them).

[261] TALLINN MANUAL, *supra* note 64, at 417.

[262] Pascucci, *supra* note 20, at 448.

Mental suffering has traditionally not seen the same level of consideration as loss of civilian life or physical injuries to civilians when considering proportionality.[263] Certainly, if an attack on a BCI would cause an incidental civilian death or injury, it would require consideration under proportionality. Yet, due to the challenge in applying causation and foreseeability—as well as difficulty of assessing and quantifying mental harm—mental suffering has not enjoyed the same level of consideration.[264] It is worth consideration that BCI making its way to the battlefield may accelerate concern of mental suffering as an incidental harm under proportionality. There is no severity requirement attached to injuries when considering incidental harm under proportionality. [265] Recognizing that an attack on a BCI could cause harm and mental injury described by neuroethicists could lead to mental suffering and harm taking greater prominence in the proportionality analysis, highlighting the clear applicability of the principle during armed conflict, when non-combatant effects are anticipated. Further, it shows that as circumstances warrant, great care must be given to analyzing the effects a given operation may have on civilians prior to its execution.

4. Humanity

Finally, the principle of humanity serves as the bedrock underlying several other IHL principles.[266] Humanity is also the complementary principle to military necessity, tempering the extent to which military necessity can be utilized to justify military operations.[267] The modern articulation of humanity is found in Article 35 of Protocol I. [268] Specifically, Article 35 notes that a state's ability to employ methods and means of warfare is not unlimited and prohibits the use of "weapons, projectiles, and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering."[269]

Adherence to the principle of humanity occurs through two main lines of effort. First, consistent with Article 36 of Protocol I, new weapon

---

[263] Gillard, *supra* note 249, at 32-33.
[264] *Id.* at 33.
[265] *Id.* at 33-34.
[266] LAW OF WAR MANUAL, *supra* note 170, para. 2.3.2 (for example, humanity "animates" safeguards for individuals who fall under the control of an adversary, protections for civilians and civilian objects, and prohibits indiscriminate weapons).
[267] *Id.* para. 2.3.1.1.
[268] AP I, *supra* note 145, art. 35.
[269] *Id.*

systems may be subject to review for compliance with IHL, specifically its compliance with humanity.[270] Next, when employed, there is an obligation to not cause undue suffering or superfluous injury.[271]

Whether the target is a person or object also affects the application of the principle of humanity. This is due to the nature of the principle and its interaction with the principle of necessity. If it is necessary to engage a target, humanity would only prevent doing so if it was done in a way specifically designed to bring about undue suffering or superfluous injury.[272] Simply engaging a legitimate military target out of military necessity, which may result in the injury or death of combatants, does not violate the principle of humanity.[273]

If a person is a lawful target, it is not a violation of IHL or the principle of humanity to engage and kill them.[274] To illustrate this point in a cyber context, consider the pacemaker scenario described in the Tallinn Manual.[275] Cyber manipulation of a pacemaker to induce cardiac arrest in a lawful target would not be a violation of humanity, but causing a series of heart attacks in order to induce pain and suffering in the target prior to killing them would be a violation of humanity.[276]

Targeting an object creates different considerations under humanity. As an illustration, should a commander determine it necessary to engage a tank, a larger munition would be required than what would be necessary to engage personnel. It is possible, or even likely, that personnel will be inside and operating the tank at the time it was struck. The larger munition could cause the adversaries inside the tank to suffer; but, because it was militarily necessary to engage the tank—and the weapon utilized was designed to destroy the tank, not to cause undue suffering or superfluous injury to the people inside—it would not violate the principle of humanity.

Brain-computer interface hardware presents unique issues in the application of humanity. While applying humanity to implanted

---

[270] AP I, *supra* note 145, art. 36; WILLIAM H. BOOTHBY, WEAPONS AND THE LAW OF ARMED CONFLICT 340-52 (2009) [hereinafter BOOTHBY, WEAPONS].
[271] LAW OF WAR MANUAL, *supra* note 170, para. 2.3.
[272] *Id.* para. 2.3.1.1.
[273] *Id.*
[274] *Id.* para. 2.3.1.
[275] TALLINN MANUAL, *supra* note 64, at 455.
[276] *Id.*

technology was contemplated by the Tallinn Manual,[277] the example of the pacemaker did not encompass the type of technology that allows for a biological system to directly interact with the cyber domain, transmit and receive data, or control military objects. Further, the potential for enduring physical, neurological, and psychological effects caused by operations against BCI presents a different dimension to the application of humanity. William Boothby indicates, as time and technological advances move forward, "[c]ultural appreciations as to which injuring mechanisms are respectively acceptable, undesirable, or abhorrent may change, affected in part by medical advance."[278] Boothby's observation is currently manifesting itself through the neuroethical discussions and advocacy surrounding BCI that highlight several of the dangers and damage to individuals' mental well-being that can be caused by attacks on BCI.

It is here that the principle of humanity will both garner outsized consideration in operations against BCI and serve an enabling function for operations against this technology. Humanity's animation of other IHL principles has already been noted in requirements and protections afforded by the principles of military necessity, distinction, and proportionality, affording protection to the brains of individuals connected to BCI. Beyond these IHL requirements directly rooted in humanity, one last layer of protection to the brains of adversaries connected to BCI is added; attacks against BCI, and by extension brains, will not be conducted in a manner designed to cause undue suffering or superfluous injury.

The concept of preventing undue suffering or superfluous injury in the conduct of operations serves the purpose of eliminating unnecessary actions to achieving a necessary military objective.[279] Thus humanity serves as a mechanism to enhance military efficiency and effectiveness.[280] Applying this concept to operations against BCI, a series of examples would serve to illustrate this interplay between military necessity and humanity.

First, consider effects on an adversary's BCI designed to gather data, share information, communicate, or exercise command and control. During armed conflict, denial or disruption of the system would serve a military purpose and would likely have the same effect as denying

---

277 *Id.*
278 BOOTHBY, WEAPONS, *supra* note 270, at 68.
279 LAW OF WAR MANUAL, *supra* note 170, para. 2.3.1.1.
280 *Id.*

information to adversaries would have today. Even if effects on this BCI would result in a psychological effect in an adversary, such as loss of confidence, these effects would— arguably— not rise to the level of undue suffering or superfluous injury. Even if they did, the valid military purpose for the operation directed at the BCI would still make the operation compliant with humanity.

But consider scenarios where an operation against BCI erases or manipulates data. Putting aside the debate on the status of data as an object of attack, if the data was associated with a military function during hostilities, an operation against this data would likely not violate humanity for similar reasons as above. If the operation targeted personal data, however, the analysis could shift. Targeting personal data, such as medical records, could manifest in unnecessarily painful physical harm if the wrong treatment was administered. Consider also the *Anon* scenario of manipulating data of painful memories, causing them to be ever present in a person's mind.[281] The result could be significant personal anguish in the targeted individual, which in turn could be considered an operation conducted simply to cause undue suffering.

Now, consider the ability to manipulate the feedback portion of the BCI cycle and how it could affect the electrical signal returning to the brain. As highlighted, this could potentially be utilized to cause physical damage to the brain or create changes in mood and personality. The military necessity of disrupting a commander's ability to make decisions or to exercise control over the battle space is certainly legitimate, but are the lasting effects of such an operation in conformity with humanity if the damage to the commander's mental well-being is permanent?

Moving to BCI designed to exert control over physical systems or individuals, potential to take actions out of conformance with the principle of humanity grow due to the physical dangers an individual may experience. Consider the example of manipulation of a person's bodily movements highlighted earlier. Imagine intelligence exists that an adversary is driving a vehicle and is equipped with a functioning BCI. Would manipulating that adversary to jerk the wheel to drive off a cliff violate humanity? Certainly, the individual would face the dual terror of loss of self-control and impending death due to the manipulation; but, they are a legitimate target.

---

[281] *See supra* pp. 4-5.

Similar scenarios endangering individuals can also be envisioned by manipulating weapon systems incorporated into the BCI. An individual utilizing a prosthetic or exoskeleton could have control seized from them, leaving them helpless and along for the ride as the new masters of the machine carry out their will. Targeting these weapon systems would serve some level of military necessity; but, an operation designed to carry out the envisaged effects would certainly have lasting effects on individuals in these systems.

The point of exploring these scenarios is to highlight the balance of military necessity and humanity. Cruelty and wonton violence are not permissible on the battlefield, only operations based on a military necessity that adhere to the other protections under IHL are permissible. Operations against BCI, including those that could result in damage to the brain, can be legally permissible; but, tempered by the ever-vital principle of humanity's protection of the brain, it will require careful application of all IHL principles.

VI. Conclusion

There is no luxury to wait for new technology to come into being before thinking about the challenges the technology will present. This article addresses one of the myriad challenges presented by BCI, fully recognizing that other open questions exist. These include the potential for intelligence collection and activity through BCI, as well as activities outside of armed conflict. While these challenges will require answers, targeting BCI during armed conflict in a manner consistent with existing IHL appears possible through a systemic evaluation of a given operation.

Brain-computer interfaces present the possibility for human beings to become more integrated with machines and computers. While this article approached this integration—or convergence—from the perspective of finding the brain's place in the cyber world, perhaps the better approach would have been to acknowledge that—as some authors contend—cyberspace is not a real place.[282] Focusing simply on operations, effects, and how they manifest in the physical world allows for clearer analysis of

[282] Robert Dewar, *Cyberspace is a Consensual Hallucination*, 6 POLICY PERSPECTIVES 1 (Apr. 2018), https://www.researchgate.net/publication/325216608_Cyberspace_is_a_Consensual_Hallucination.

the application of IHL and consideration of the concerns of neuroscientists and neuroethicists.

The concerns of neuroethicists reflect in many ways how convergence with technology, and envisioning a separate cyber or technical world, seems to be slowly stripping our humanness away. Our brains are the last great step in this integration, and our neuroethicists have—rightly—sounded the alarm on possible repercussions on the path ahead. The alarm is all about the human, not the machine, a point that should be central in any discussions about such technology. We should therefore be sensitive in our legal analysis to preserving the humanness of persons connected to machines, which will naturally allow for IHL principles—specifically the principle of humanity—to provide protection from the dangers created by man-machine convergence technologies such as BCI.