MEANS, METHODS, AND MACHINES: CLASSIFYING TECH-ENABLED TERROR UNDER IHL AND ICL

Harsh Mahaseth[*]

ABSTRACT

Terrorist actors increasingly mobilise artificial intelligence, human enhancement and other advanced technologies, straining weapon-centred legal categories. This paper asks when Artificial Intelligence systems and bio-enhanced capabilities qualify as "weapons, means or methods of warfare" under Additional Protocol I and how Article 36 weapons-review duties apply when the instrument is partly human and partly technological. It evaluates downstream implications for the International Humanitarian Law principles of distinction, proportionality and unnecessary suffering; situates enhancement within the Biological and

[*]Harsh Mahaseth is an Associate Professor, Jindal Global Law School and Academic Visitor, Institute of South Asian Studies, National University of Singapore. The author can be reached out at hmahaseth@jgu.edu.in.

Toxin Weapons Convention and Chemical Weapons Convention; and integrates International Human Rights Law concerns over consent, bodily integrity, privacy and data security, including guidance from UNESCO bioethics norms. Turning to accountability, the paper maps International Criminal Law pathways, individual liability, aiding and abetting (Article 25(3)(c)), command responsibility (Article 28) and negligence-based theories, while addressing autonomy-driven responsibility gaps. It proposes a practical classification approach and a regulatory–criminalisation pathway that recognises certain enhancements and Artificial Intelligence's use as "weapons," extends ex ante reviews and dual-use safeguards, and specifies ex post modes of liability for designers, deployers and commanders. The result is a coherent template for governing technology-enabled terrorism across International Humanitarian Law, International Human Rights Law, and International Criminal Law.

Keywords: *Terrorism, Artificial Intelligence, International Humanitarian Law, International Human Rights Law, International Criminal Law, Liability.*

I. INTRODUCTION

There has been a spike in terrorist activities worldwide and news tabloids are filled with cases of violence spurred by terrorism. Adding to this threat, automated tasks performed using Artificial Intelligence (AI) can potentially increase the scale and impact of these attacks, especially when carrying out cyberattacks. Gone are the days when terrorism was limited to unleashing bullets upon people and buildings. In recent years, most terrorist attacks in Europe have been perpetrated not by using new technology, but by low-technological means, such as large-scale explosions or mass shootings, and involving easily accessible items used as weapons, such as cars, trucks, knives, and guns.[1] With technological advancements, drones can now cause much more destruction than the small drones did in the Syrian battlefield in

[1] David Parker, Julia Pearce, Lasse Lindekilde, and M Brooke Rogers, '*Challenges for Effective Counterterrorism Communication: Practitioner Insights and Policy Implications for Preventing Radicalization, Disrupting Attack Planning, and Mitigating Terrorist Attacks'* (2019) 42(3) *Studies in Conflict & Terrorism* 264, 264-291 https://pure.au.dk/portal/en/publications/challenges-for-effective-counterterrorism-communication-practitioner accessed 29 July 2024.

2018.[2] Various gadgets and logistics have become available, enabling terrorists to devise new ways of causing upheaval and destruction to public property and infringing on the right to life of many innocent civilians. The use of AI in terrorism has led to a pressing need for regulation.

It is plausible that terrorist groups will exploit AI for their own benefit. Just like the rest of society, terrorists are likely to benefit from technology and AI, using it for military operations and intelligence collection. Automated tasks performed using AI can potentially increase the scale and impact of these attacks, especially in carrying out cyberattacks.[3] The condition that appears to fear and fascinate individuals the most is that of AI robots. Scenarios often depict sentient, killer robots with abilities mimicking the human brain but lacking human inhibitions. The Metaverse, a new (virtual) reality, has become a breeding ground for cyber-terrorism where terrorists can plot and execute their plans while representing their virtual selves. The Global Security Pulse warns not only of scenarios involving armed AI robots but also of 'terrorist drone swarm' scenarios.

An online YouTube video posted in 2017 called 'Slaughterbots,' which has generated over 3 million views, portrays a dystopian scenario

[2] Scott Crino and Andy Dreby, '*Turkey's Drone War in Syria: A Red Team View'* (16 April 2020) *Small Wars Journal* https://smallwarsjournal.com/jrnl/art/turkeys-drone-war-syria-red-team-view accessed 29 July 2024.

[3] Miles Brundage, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe, and others, *'The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation'* (February 2018) University of Cambridge https://doi.org/10.17863/CAM.22520 accessed 29 July 2024.

where vast swarms of small armed drones are created by an unidentified government to destroy civilians.[4] Although the advocacy group 'Stop Autonomous Weapons' developed and uploaded the video with the political intent of preventing military use of unmanned weapons, this video easily entered the debate on terrorist use of technology.[5] The 'killer drone swarms' scenario is related to proof that ISIS has used consumer-grade small drones on the Syrian battlefield armed with grenades, pointing to a likely scenario of the horror we may face.[6]

AI has the potential to amplify the scale and impact of terrorist activities. Automated systems can be used to orchestrate large-scale cyber-attacks, disrupt critical infrastructure, and execute complex operations with minimal human intervention. For example, AI algorithms can optimize the timing and coordination of attacks, making them more efficient and harder to detect.[7] Alongside AI and drones, the use of the Internet by extremists warrants attention. Terrorists employ digital technologies for propaganda and messaging, often using

[4] *Stop Autonomous Weapons*, 'Slaughterbots' (13 November 2017) YouTube <https://www.youtube.com/watch?v=6KjX8EF95w4> accessed 29 July 2024.

[5] Jason Ware, 'Terrorist Groups, Artificial Intelligence and Killer Drones' (24 September 2019) *War on the Rocks* <https://warontherocks.com/2019/09/terrorist-groups-artificial-intelligence-and-killer-drones/> accessed 29 July 2024.

[6] Daveed Gartenstein-Ross, 'Terrorists Are Going to Use Artificial Intelligence' (3 May 2018) *Defense One* <https://www.defenseone.com/ideas/2018/05/terrorists-are-going-use-artificial-intelligence/147944/> accessed 29 July 2024.

[7] Marcus Comiter, '*Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It'* (Belfer Center for Science and International Affairs, Harvard Kennedy School 2019.

anonymous forums and benefiting from end-to-end encryption and virtual private networks (VPNs), which shield their identities and intentions.

Computer and networking advances have made new forms of operations feasible for a larger range of radicalized individuals. Widespread internet connectivity,[8] end-to-end encryption,[9] and VPNs[10] have enabled terrorists to remotely inspire and coordinate attacks. These operations require no extensive preparation or logistical planning and can be carried out by anyone, anywhere, using crude instruments such as knives or vehicles. Encrypted messaging systems like WhatsApp and Telegram provide users with anonymity by scrambling data, preventing law enforcement from accessing or intercepting these messages.[11] This advancement in the digital space raises fears about the amalgamation of these technologies with humans,

[8] Michael Steinbach, '*ISIL Online: Countering Terrorist Radicalization and Recruitment on the Internet and Social Media*' (6 July 2016) Statement before the Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations, Washington DC <https://www.fbi.gov/news/testimony/isil-online-countering-terrorist-radicalization-and-recruitment-on-the-internet-and-social-media-> accessed 29 July 2024.

[9] Robert Graham, '*How Terrorists Use Encryption*' (May 2016) 9(6) *CTC Sentinel* 20, 32 <https://ctc.usma.edu/posts/how-terrorists-use-encryption> accessed 29 July 2024.

[10] *EUROPOL Public Information*, *Changes in Modus Operandi of Islamic State Terrorist Attacks* (2016) The Hague.

[11] Robert Graham, '*How Terrorists Use Encryption'* (May 2016) 9(6) *CTC Sentinel* 20, 20.

highlighting the need for an international framework to address these emerging threats.

II. ENHANCED HUMAN TECHNOLOGY AS WEAPONS UNDER THE GENEVA CONVENTION

First, the examination of the Additional Protocol I of the Geneva Convention raises the question: "Does human enhancement (HE) fall under Article 36?" This Article could imply that war fighters themselves might be categorized as 'weapons'. A crucial aspect to understand is whether entities other than traditional weapons are subject to scrutiny under this Article. International law lacks a specific definition for 'weapon'. Article 36 refers to 'weapons, means and methods of warfare'. A weapon could be defined as something designed to target a military objective or enemy combatant, aiming to destroy or reduce the effectiveness of the target or incapacitate the enemy combatant.[12] Historically, animals like dogs, elephants, and dolphins have been used in warfare. Today, dogs are trained for police and military roles due to their specialized skills. If autonomous robots are considered controlled weapons, what about humanoids with robotic components? As humans replace body parts with robotic elements, they

[12] International Committee of the Red Cross, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977* (ICRC 2006) <https://www.icrc.org/en/doc/assets/files/other/irrc_864_icrc_geneva.pdf> accessed 29 July 2024.

become increasingly mechanized. The question then arises: when does a human become a robot, and thus a weapon? Enhancements such as amphetamines for focus or drugs for stamina could blur this line, raising ethical concerns about human augmentation in warfare.

A critical factor in this discussion is the distinction between 'automated' and 'autonomous'. Automated weapons function on a pre-programmed set of commands, making their outcomes more predictable. In contrast, autonomous weapons equipped with AI can learn and adapt, resulting in less predictable outcomes. The degree of human intervention plays a significant role in determining the level of autonomy.[13] This consideration is also relevant for combatants who are part human and part robot.

Various countries approach the classification of autonomous weapons differently. For instance, the U.S., France, and Germany define autonomous weapons as those capable of selecting and attacking targets without human intervention once activated.[14] China, Estonia,

[13] S Saini and P Dominic, Chapter 1: Background and Definitions in '*Legal and Policy Implications of Autonomous Weapons Systems'* (The Centre for Internet and Society 2020) 9 <https://cis-india.org/internet-governance/legal-and-policy-implications-of-autonomous-weapons-systems> accessed 29 July 2024.

[14] U.S. Department of Defense, *Directive No. 3000.09, 'Autonomy in Weapons'* (2012) AI Regulation, 'French Defense Ethics Committee's Opinion: Need for a Clear Distinction Between LAWS and PLAWS' (2021) <https://ai-regulation.com/french-defense-ethics-committees-opinion-about-laws-and-pawls/> ;Federal Foreign Office, '*German Commentary on Operationalizing All Eleven Guiding Principles at a National Level as Requested by the Chair of the 2020 Group of Governmental Experts (GGE) on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems (LAWS) within the Convention on Certain*

and Finland focus on characteristics such as lethality, autonomy, impossibility of termination, indiscriminate effects, and evolution.[15] Human intervention is a common factor in these definitions, which is crucial for assessing the level of autonomy. These parameters provide insight into the characteristics and functioning of autonomous weapons and how humanoids might be classified. However, the act of making final decisions and taking actions rather than merely observing and orienting is what fundamentally differentiates autonomous systems.

A pragmatic approach is to consider humans as weapons from the outset, thereby avoiding the complex issue of determining when they become weapons. A combatant with robotic implants, such as machine guns or lasers, is clearly weaponized, possessing capabilities that can be incapacitating or destructive.[16] The Cambridge Dictionary defines 'weapon' as "an object used in fighting or war, such as a gun or a bomb,

Conventional Weapons (CCW)' <https://documents.unoda.org/wp-content/uploads/2020/07/20200626-Germany.pdf> accessed 29 July 2024.

[15] Brian Stauffer, '*Stopping Killer Robots: Countries' Positions on Banning Fully Autonomous Weapons and Retaining Human Control* (Human Rights Watch 2020)' <https://www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and> accessed 29 July 2024.

[16] U.S. Army Combined Arms Center, '*Robots on the Battlefield: Contemporary Issues and Implications for the Future'* (Combat Studies Institute 2014) <https://apps.dtic.mil/sti/pdfs/ADA605889.pdf> accessed 29 July 2024.

or something used against someone."[17] Additionally, the Merriam-Webster describes it as "something used to injure, defeat, or destroy."[18]

These definitions suggest that humans and attack dogs could be regarded as weapons. If humans are considered weapons from the beginning, there is no need to pinpoint when human enhancement transforms them into weapons. Thus, soldiers could be viewed as 'weapons' themselves. This perspective avoids the problematic task of drawing a line between enhanced humans and weapons, as even simple enhancements or unarmed combat might render a person a weapon under these definitions. This approach aligns with dictionary definitions, where objects or beings used in combat are classified as weapons, confirming that both normal soldiers and attack dogs could be considered weapons from the outset.

A legal review under Article 36 includes any modification to an existing weapon that alters its function or any weapon previously reviewed but subsequently modified. Consequently, Article 36 would encompass enhanced humans, simplifying the development of a legal framework for human enhancement and advanced weapon technologies. If enhanced humans are deemed weapons under Article 36, what are the implications? Historically, modern weapons and

[17] *Cambridge University Press*, 'Weapon' in *Cambridge Advanced Learner's Dictionary & Thesaurus* <https://dictionary.cambridge.org/dictionary/english/weapon> accessed 15 May 2022.

[18] *Merriam-Webster*, 'Weapon' in *Merriam-Webster Dictionary* <https://www.merriam-webster.com/dictionary/weapon> accessed 15 May 2022.

techniques must meet at least the following criteria: (1) the principle of distinction; (2) the principle of proportionality; and (3) the prohibition of causing excessive damage or unnecessary suffering. The principle of distinction mandates that a weapon must discriminate between combatants and non-combatants.[19] For example, chemical agents and anti-personnel landmines are considered indiscriminate and unconstitutional as they do not differentiate between a civilian and an enemy combatant. The principle of proportionality requires that the use of force be commensurate with the strategic objective, aiming to minimize civilian casualties. Lastly, the prohibition of unnecessary suffering ensures that weapons must avoid inflicting excessive damage or pain beyond what is necessary to incapacitate a fighter. This prohibition has led to bans on weapons like poison, explosive bullets, and blinding lasers, which cause excessive harm. For now, if we disregard enhancements intended for use against enemies, such as mood-altering drugs to calm a crowd or truth-enhancing substances for interrogation techniques, the former would be banned by the Chemical Weapons Convention due to its indiscriminate nature, while the latter might be prohibited under rules against torture and mistreatment of prisoners.

[19] Diakonia International Humanitarian Law Centre, '*The Principle of Distinction'* <https://www.diakonia.se/ihl/resources/international-humanitarian-law/principle-of-distinction-protection-of-people-and-objects/> accessed 29 July 2024.

III. INTERNATIONAL FRAMEWORK FOR BIOLOGICAL WEAPONS AND HUMAN ENHANCEMENT

Second, the question is "Whether human enhancement falls under the Biological and Toxin Weapons Convention (BTWC) as a biological weapon". Article I reads as follows:

"Each State Party to this Convention undertakes never in any circumstances to develop, produce, stockpile or otherwise acquire or retain: (1) microbial or other biological agents, or toxins whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes; (2) weapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict."

The BTWC, though, is silent on the question of human enhancement falling under the term biological weapons; unpredictable advances in genetic engineering, biotechnology, synthetic biology, and other research areas are expected. However, the conventional belief is that all these "agents" are limited to being approximately microbial in size and to biological substances that are aimed at enemies, not targeted at enhancing one's own military personnel.[20] Regrettably, this statement is not sufficiently clear in the BTWC; that is to say, it does not describe what a biological agent is. Agents may also be biological agents, like anthrax, caused by Bacillus anthracis, that are indiscriminate and

[20] *'The Biological Weapons Convention'* <http://bwc1972.org/home/the-biological-weapons-convention/> accessed 29 July 2024.

challenging to control as weapons. The bacterium forms tough spores that persist for long periods and can be carried by the wind, infecting children or entire populations as easily as soldiers. This violates the principle of distinction in International Humanitarian Law (IHL). When conditions are suitable, such as inside human lungs, the spores germinate and release life-threatening toxins, highlighting the persistent and uncontrollable nature of anthrax as a biological weapon.[21] Similarly, agents may also be entities in a wider yet more coherent context (e.g., a government informant is a 'secret agent'). If so, then agents will become improved war fighters. Even if this concept is denied and it is stipulated that biological agents must be non-personal substances, a concept not clear in the BTWC, they can still treat the technology of enhancement itself as an agent, apart from the war fighter it enhances.

In addition to the BTWC, the usage of chemicals can also be considered as a method of warfare under the Chemical Weapons Convention ('CWC'). Article II (1) of the CWC defines chemical weapons in the way of toxic chemicals and their precursors, and munitions and devices. It specifically elaborates on the usage of chemicals in designing the devices that cause death. Similarly, Clause IV, which defines the 'key component of a binary or multi-component chemical system', prohibits the use of chemicals that take part at any stage of

[21] David P Clark and Nanette J Pazdernik, '*Biological Warfare: Infectious Disease and Bioterrorism' (2016) 16 Biological Warfare and Bioterrorism 687, 687-719'* <https://doi.org/10.1007/s12345-016-7890-y> accessed 29 July 2024.

production and play an important role in determining the toxic properties of the final product.[22] Thus, we can conclude that even the chemicals that are used in the production or assembling of the device or which result in human enhancement, consequently leading to their weaponization, are under the ambit of the CWC.

IV. BIOETHICS AND HUMAN RIGHTS FOR HUMAN ENHANCEMENT TECHNOLOGIES (HET)

Third comes the International Human Rights issue. Human Rights cannot be ignored when we are talking about human enhancement. Torture and cruel, inhumane or degrading treatment are forbidden by Article 5 of the Universal Declaration of Human Rights ('UDHR') and Article 7 of the International Covenant on Civil and Political Rights ('ICCPR').[23] They imply, in fact, a restriction on the execution of medical or experimental research without free consent. No person shall, under Article 12 of the UDHR and Article 17 of the ICCPR, be subjected to arbitrary or unlawful interference with his or her privacy.[24]

[22] Organisation for the Prohibition of Chemical Weapons, *Chemical Weapons Convention* art II (IV) <https://www.opcw.org/chemical-weapons-convention/articles/article-ii-definitions-and-criteria> accessed 29 July 2024.

[23] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) art 5; International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) art 7.

[24] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) art 12; International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) art 17.

Neither of the General Comments to the two sections of the ICCPR allows any reference to science nor relates to the prospect of scientific or technological abuses of such rights. However, it is highly conceivable that, depending on the degree of intrusiveness, compulsory enhancement will infringe on one or both of the two sections. Provisions that guarantee privacy protection are widely applicable to the cybersecurity challenges posed by HETs, such as data leaks, denial-of-service attacks and unauthorised access to implants.

Article 12, which acknowledges the right of all to enjoy the highest achievable level of physical and mental fitness, is contained in the applicable provisions of the International Covenant on Economic, Social and Cultural Rights (ICESCR).[25] All health facilities, goods and services must recognise medical ethics and also be culturally appropriate, i.e. considerate of the culture of minorities and other communities, gender-sensitive and life-cycle-sensitive, along with being respectful of their confidentiality and improving the health status of those concerned.[26] This right includes freedoms, and the same much like any other right, comes with entitlements.[27] Accordingly, the right to health is closely connected to the concept of liberty, freedom of choice and limitations thereof, as well as to protection, consistency

[25] Convention on the Elimination of All Forms of Discrimination against Women (1979) art 11.1(f) and 12, International Convention on the Elimination of All Forms of Racial Discrimination (1965) art 5(e)(iv), Convention on the Rights of the Child (1989) art 24.

[26] Universal Declaration on Bioethics and Human Rights (2005) art 12.

[27] Universal Declaration on Bioethics and Human Rights (2005) art 11.

and care requirements that are of crucial importance to the regulation of HETs. However, the precise scope of this right lies under the vast jurisdiction of the State, which determines how scarce services can be distributed.

Under Article 15.1 (b) of ICESCR, the states are bound to the rights of individuals "to enjoy the benefits of scientific progress and its applications". Para 2 of the same article directs the states to ensure complete fulfilment of this to include those required for the protection, creation and propagation of science and culture. A point of contention continues to be what constitutes 'benefits'. The definition of this word has traditionally tended to concentrate on cultural involvement in the advancement of science, whether through funding for research projects or through the creation of ways of disseminating and transmitting the findings of scientific research. In the area of cultural freedom, the UN Special Rapporteur "[t]he words 'benefits' of research and 'scientific progress' convey the notion of a positive effect on people's well-being and the realisation of their human rights".[28] The right to profit from scientific advances remains widely underdeveloped, although, in recent times, it seems to have received greater discussion and focus.

Finally, the UNESCO Declaration on Bioethics and Human Rights discusses ethical issues pertaining to "medicine, life sciences and associated innovations as applied to humans." For the basic explanation

[28] Farida Shaheed, '*Report of the Special Rapporteur in the Field of Cultural Rights: The Right to Enjoy the Benefits of Scientific Progress and Its Application*' (2012) section III A.24.

that HE concerns improvements in the human body, the problems posed by HE will be bioethical in nature. For the purpose of the Declaration, bioethics has been defined in the explanatory memorandum as "a systematic, pluralistic and interdisciplinary field of study involving the theoretical and practical moral issues raised by medicine and life sciences as applied to human beings and humanity's relationship with the biosphere".[29] In the regulation of HE, many principles of the Declaration should be taken into account. States have a duty, in particular, to protect the privacy of individuals and the security of their personal records.[30] The need to maintain the secrecy of data relating to and created by the human body is of special significance in view of the safety issues relating to HETs. In addition, encouraging health and social progress must be a primary priority of governments.[31] The same clause recalls that among these basic rights of any human being is the right to enjoy the highest attainable quality of health and that developments in science and technology can advance, among other things, the development of living standards and the environment.[32] In addition to that, the States should ensure that the benefits of all scientific findings are shared, along with their application to society as a whole, in addition to being shared within the

[29] UNESCO, *Explanatory Memorandum on the Elaboration of the Preliminary Draft Declaration on Universal Norms on Bioethics* para 17.

[30] Universal Declaration on Bioethics and Human rights (2005) art 9.

[31] Universal Declaration on Bioethics and Human rights (2005) arti 14(1).

[32] Universal Declaration on Bioethics and Human Rights (2005) art 14(2).

international community.[33] Here, "benefits" can assume the shape of access to healthcare services; the availability of new research-based diagnostic and therapeutic modalities or products; or health service funding.

Fully autonomous weapons are a critical concern in military technology, necessitating thorough examination under the Martens Clause. This international humanitarian law provision ensures protection for civilians and combatants when specific treaties are absent. The Clause applies to fully autonomous weapons because they are not specifically addressed by international law, providing key factors for states to consider as they evaluate such emerging technologies. Its principles of humanity and dictates of public conscience demand a pre-emptive ban on the development, production and use of these weapons. After initial expert meetings, the Convention on Conventional Weapons (CCW) began formal discussions in 2017, with around 80 states convening again in August 2018.[34]

With the analysis so far, it can be rightly concluded that IHL can provide for the classification and the framework to uphold human rights when HE technologies turn into potential weapons. However, it is important to look at it in the light of International Criminal Law

[33] Universal Declaration on Bioethics and Human rights, (2005) art 15.

[34] Human Rights Watch, 'Heed the Call: A Moral and Legal Imperative to Ban Killer Robots' (21 August 2018) <https://www.hrw.org/report/2018/08/21/heed-call/moral-and-legal-imperative-ban-killer-robots> accessed 29 July 2024.

(ICL) so that the accountability for terrorism through such advanced technologies by terrorist organizations can be construed.

V. TERRORISM THROUGH ADVANCED HUMAN TECHNOLOGIES AND THE INTERNATIONAL CRIMINAL LAW FRAMEWORK

The IHL puts the onus and sanctions on the state to uphold Human Rights, but when it comes to the use of AI in Terrorism, it is important to look at ICL to understand the mechanism of liability and how it can provide a framework for the use of advanced technologies. The current legal framework, with the underlying principles of Laws of Armed Conflict ('LOAC') as a measure to control terrorism, needs to be reflected upon if we want to include HE and other advanced technologies. A number of questions that arise while deciding the liability under the ICL are regarding the accountability, liability of humans, developer accountability, nature of war crimes, etc. Thus, the classification of terrorist activities using enhanced technologies needs to be analysed under the present laws.

Individual Criminal Liability, which is considered to be the foundation of ICL after the Nuremberg Trial, makes the terrorists using enhancement technologies liable for war crimes.[35] As the Nuremberg

[35] Edoardo Greppi, 'The Evolution of Individual Criminal Responsibility under International Law' (1999) 835 *International Review of the Red Cross* <https://www.icrc.org/en/doc/resources/documents/article/other/57jq2x.htm> accessed 29 July 2024.

Trial specifically laid down that crimes are to be committed by humans and not abstract entities, the human enhancement that is done using AI would result in the classification of the crimes as war crimes.[36] While the absence of human oversight in autonomous weapons leads to the question of "who" should be held accountable for the crime, terrorism through HE has the assumption that the 'who' could be any organization or individual. However, it leads to the possibility of accountability of the developer. It is important for the LOAC to apply that an armed conflict should take place. However, in the case of the development of technology such as software and tool programming, it is very much possible that the 'weapons' came into existence long before the conflict commenced, resulting in detaching the conduct of the developer from the conflict and providing a *de facto* immunity.

The way out of the loop can be the Art. 25(3)(c) of the Rome Statute, which criminalizes aiding, abetting or providing assistance in the commission or attempted commission of the crime. However, preceding that, it is important to establish the *mens rea* of the developer as well. In accordance with Art. 30 of the Rome Statute, the developer's intention to facilitate the commission of a crime will have to be proved. Thus, the developer could not be held liable even if they were aware of the perpetrator's intention and knowledge that their product could assist in the commission of an offence if the technology is developed

[35] *The Trial of the War Criminals before the International Military Tribunal Nuremberg Judgment* (1 October 1946).

with the sole aim of profiteering.[37] The accountability gap can be bridged if the *mens rea* and the *actus reus* are amended and interpreted in such a way as to bring the ex-ante actions of the individuals under their ambit.

Another principle that can potentially govern the terrorism of advanced technologies is the Doctrine of Command Responsibility. Article 28 of the Rome Statute talks about the Doctrine of Command Responsibility, where military commanders can be held responsible for the actions of their subordinates. An important component of the Doctrine of Command Responsibility is the presence of effective control of the commander over the subordinate, i.e. the commander or the superior authority oversees the actions and has the power and chance to prevent any kind of damage.[38] When terrorists use enhanced technologies or any kind of HE which results in war crimes, the doctrine of Command Responsibility can be applied to establish a relationship between the system and the superior authority that controls the system. Even in the case of HE, when the involvement of human intelligence is such that the actions or the usage of the technological enhancement is such that the person using it or having the command over it knows that it will result in the commission of a war crime, liability exists. This way, the terrorist organizations that have deployed such technologies or

[37] S Saini and E Elizabeth, '*Legal and Policy Implications of Autonomous Weapons Systems'* (The Centre for Internet and Society 2020) 50.

[38] *Prosecutor v Delalić et al.* (Čelebići case) Judgement, Case No IT-96-21-T, T Ch II, 16 November 1998.

individual terrorists who use enhanced human technology and are working under the control of larger organizations, can be held liable. While it is true that the technology or the weapon itself cannot be attributed to the willingness to commit a crime, the presence of human intelligence in HE or even the knowledge that the system is manufactured in a way to commit a crime is sufficient to establish liability. The Doctrine of Command Responsibility thus makes the person who is either using the enhanced technology himself or using that as a weapon through another to commit war crimes or even having the constructive knowledge of it, liable under the Rome Statute.

When it comes to cybercrime and terrorism through AI, the responsibility falls on the manufacturers of such software or the person who owns the technology.[39] The reason behind it is that the AI cannot be given the human attributes of mental state and actions pursuant to criminal intentions. However, when it comes to enhanced humans, they have both the mental state of a human being and the capability to commit crimes like that of an AI system. But when we talk about war crimes through enhanced technology, there exists a high possibility of negligence and malfunction in the enhanced technology. Though negligence imposes a liability at the fault of the defendant, the complexity lies in determining the standard of care.[40] Further, to set the negligence-based liability, it is important to establish that the damage

[39] Nora Osmani, *'The Complexity of Criminal Liability of AI Systems'* (2020) 14(1) *Masaryk University Journal of Law and Technology* 61, 53-82 https://doi.org/10.5817/MUJLT2020-1-3.
[40] ibid.

caused was foreseeable and that the manufacturer or the user could have anticipated the potential malfunction. However, we cannot ignore that enhanced humans or other enhanced technologies have the self-learning capacity and autonomy, which makes their actions and outcomes unpredictable.[41] Therefore, it will be difficult to shift the liability all upon the owner of the technology, as the extent of the 'duty of care' will become hard to determine. Moreover, AI can also be used in terrorism through the means of lethal autonomous robots (LARs). LARs lack moral autonomy and responsibility. Creating a moral agent requires strong AI with human-like intelligence, intentions, reflection, and consciousness. Current AI systems learn unpredictably, creating a "responsibility gap", where programmers lose control over the AI's actions. As AI systems use complex logic and learning processes, they act beyond their creators' observation, making manual intervention impossible. Therefore, accountability should not be attributed to the AI or its creators, as autonomous systems operate independently and unpredictably. This underscores the challenge of managing and regulating truly autonomous machines.[42] It results in a loophole for the terrorists to circumvent the liability. A possible solution to this is the recognition of enhanced humans as weapons which will make their

[41] A Conn, *'The Risks Posed By Lethal Autonomous Weapons'* (4 September 2018) *Future for Life* <https://futureoflife.org/2018/09/04/the-risks-posed-by-lethal-autonomous-weapons/> accessed 29 July 2024.

[42] Heather M Roff, *'Killing in War: Responsibility, Liability and Lethal Autonomous Robots'* in F Allhoff, N G Evans, and A Henschke (eds), *Routledge Handbook for Ethics and War* (Routledge 2013).

actions inherently dangerous and thus manufacturers and the owners/users of such technology and weapons will have strict liability even if the initial motive of the manufacturer or the user was to not commit a war crime. Their subsequent actions will result in holding them accountable as they will have the liability to take preventive measures.

VI. CONCLUSION

The constant development of technology, whether through the making of a virtual world such as the Metaverse or technology delving into human lives through humanoids, has only led to the greater need for regulation. Further, the use of enhanced technology in terrorism and the ways in which cyberterrorism is taking new forms make it the right time to curate the legal framework and regulate it in the upcoming digital world. The involvement of human enhancement and other advanced technologies in terrorism goes beyond war crimes through arms and ammunition and poses bigger questions of their regulations through current laws, human rights violations, and how they will be criminalized under the international legal framework.

The weaponization of technology through the human body lies at the junction of IHL and ICL, which establishes the argument of the present paper, which is to recognise them as "weapons" under the IHL. By including technological enhancement through robotic mechanisms and chemicals under the ambit of "weapons" in the Geneva Convention and

Chemical Weapons Convention, along with the BTWC, criminalizing their use in terrorism becomes easier. Since the enforcement of ICL requires the commission of war crimes or crimes against humanity, recognition of humanoids or other advanced technologies as weapons will make terrorist organisations or even individual terrorists inherently liable for their usage. The most important aspect highlighted throughout the research is the potential of the current international legal framework to deal with war crimes and terrorism through such human advancement technologies. The classification of advanced technology as 'weapons' and understanding of the bio-ethical issues with respect to bodily autonomy and privacy, along with criminalizing its usage in terrorism, will help in making the correct legal pathway from the very beginning. Eventually, the entire legal framework for the alliance of Human and Artificial Intelligence, which will soon be leading the future wars, can be made on the foundation that will be laid through such classification.