



COMMAND RESPONSIBILITY IN THE AGE OF ALGORITHMS: CRIMINAL LIABILITY FOR AI-ORIENTED CYBER OPERATIONS

Article History:

Name of Author:

Gursharan Kaur¹

Affiliation: ¹ Ph.D. Scholar

Corresponding Author:

Gursharan Kaur

Email: s.gursharankaur@gmail.com

Received: 12-01-2026

Revised: 05-02-2026

Accepted: 20-03-2026

Published: 03-04-2026

This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution-Noncommercial-Share Alike 4.0 License, which allows others to remix, tweak, and build upon the work non-commercially, as long as appropriate credit is given and the new creations are licensed under the identical terms.

Abstract: Background: Artificial Intelligence (AI) is rapidly transforming the conduct of cyber operations and attacks in the battlefield by interfering in the process of decision-making by military commanders. These advanced technologies have enabled top-notch speed, scale and immense complexity in the cyberspace. On one hand, such technologies have increased the State's reliance on machine and algorithm-oriented systems to identify threats, reach precise targets, deploy countermeasures and execute cyber operations in context of cyber warfare but on the other hand, the risk of harm to civilian objectives and disproportionate attack/counter measures- resulting in damages to civilians and those who are not a part of the hostilities- has grown dangerously and tremendously. This research paper centrally examines the relationship between AI, cyber warfare, International Humanitarian Law (IHL) and International Criminal Law (ICL). It studies the impact of AI on cyber operation and attacks launched on the battlefield with regard to the central rules and principles of IHL. Along with this, the paper also examines the individual criminal responsibility, i.e., the military commander's responsibility under the realms of International Criminal Law (ICL). Further, the paper focuses on the applicability of core ICL doctrines, such as command responsibility, superior responsibility, aiding an attack, and so on. It studies whether the military commander's decisions based and relied on systems run by machines and algorithms meet the standards of "mental element" under the Rome Statute. This paper argues that any such violations by the use of AI in an Armed Conflict result in war crimes and should be addressed according to the rules and principles of IHL. And with regard to ICL, the paper contends that the traditional concept of command responsibility, which centrally focuses on human decision-making and intent, fails to deal with situations wherein the decisions are made on the basis of algorithms and AI-oriented systems. The author emphasises on the urgent need to reconsider and re-develop the concept of command responsibility which aligns with the modern-day technologies run on the agencies of AI and bridge this legal gap under ICL.

Keywords: Cyber Warfare, Artificial Intelligence, International Humanitarian Law, International Criminal Law, Command Responsibility.

INTRODUCTION

With time, the weaponry and mode of warfare have significantly evolved marking a shift from clashes between different States and combatants to non-state conflicts and civilians being more targeted during a declared situation of armed conflict, whether willingly or otherwise.

Artificial Intelligence (hereinafter, referred to as AI)

oriented cyber operations are basically those operations which can choose, attack or capture targets on the battlefield without meaningful human interaction and intervention. Currently, the use of AI-oriented cyber operations in the context of military and their adoption is quite exaggerating and requires ethical evaluation as well as judgment. Such applications may include targeting precise military targets, detecting drones, providing humanitarian aid,

monitoring and surveillance. But these operations have the tendency to impact the chain of command due to their ability to make decisions on their own based on algorithms. In case of traditional warfare, the military commander is expected to discipline the troops but in case of cyber operations which meet the threshold of an armed conflict and are based on automated AI- oriented system, the question of command responsibility comes into play.

The central question that arises is how such AI-oriented cyber operations be dealt under the exigencies of International Humanitarian Law (hereinafter, referred to as IHL) i.e., the *lex specialis*, special law applied in all the scenarios of a declared armed conflict. This branch of International Law deals with the means and method of warfare and conduct of hostilities in the times of war. Therefore, it is essential that use of any AI-oriented systems should be in accordance with the rules and framework of IHL. Another important consideration comes from the domain of International Criminal Law (hereinafter, referred to as ICL), which includes the assignment of culpability for actions undertaken by such AI-oriented systems resulting in cyber operations meeting the threshold of an armed conflict. A concrete concern revolves around the notions of attributing responsibility to any such action taken by the military commander on the battlefield with the assistance of an AI-oriented system in case of any discrepancies or unanticipated consequence of such a military act. There exists a “responsibility gap” as to who should be held responsible for such a violation of IHL i.e., the military commander, the AI system, the developer, the manufacturer, the State or the programmer? The notions of mental element or *mens rea* as required for the purposes of the Rome Statute dealing with the rules of ICL cannot be met in case of an AI-oriented system as they are completely based on composite databases and algorithms. So, such military operations are executed often without or with negligible human intervention and leads to the thread between human intellect-based decisions and military action to be cut off.

This paper essentially bridges the gap between IHL and ICL principles in the context of the military commander’s responsibility and deals only with his “mental element” clause under the notions of Rome Statute. The paper argues that the traditional concept of *mens rea* fail to deal with the current means and methods of warfare wherein the decisions of the military commander may be based on AI-oriented systems and which may in consequence violate the central rules and principles of IHL. There is a stringent accountability gap created by the virtues of autonomy and automation on the battlefield. The limitation of this research includes the non-inclusion of the central principles of IHL. The sole focus is on the concept of “Command Responsibility” under ICL.

The research methodologies include the descriptive approach dealing with the present state of affairs in the field of ICL and AI-oriented systems. Also, analytical approach which highlights the legal and ethical challenges incurred due to the utilisation of AI on the battlefield by the military commander in his decision-making processes.

I. AI AND CYBER OPERATIONS: OVERVIEW AND RELATIONSHIP

AI is a “multidisciplinary field of computer science that focuses on creating machines capable of performing tasks that typically require human intelligence i.e., aims to simulate human cognitive functions like learning, problem-solving, perception, and situational understanding.” There is no concrete definition of AI as it encompasses all the spheres of technology and advancements. To state in simpler terms, there are two variants of AI that exists prominently. Firstly, Narrow AI or weak AI that is built for just a specific task or job. It is trained to perform that particular tasks but lacks in applying cognitive functions of human intelligence. Secondly, General AI or strong AI which poses the ability to function according to cognitive abilities of human intelligence and is capable of understanding, learning and doing situational analysis. Such AI is enabled to use logical reasoning and make prompt decisions. They analysis the situation, refer to their databases and make decisions according to algorithms.

The interplay between AI and Cyber Operations takes into its realm few areas wherein AI is used in the cyberspace. For example, Cybersecurity wherein AI can essentially be used to detect and also prevent any cyber threats that may exist by analysing patterns in network traffic and any pin pointing any abnormalities in the cyberspace. It can easily bring to surface any cyber-attacks or operations and stop them in real-time. Another example includes Data Analytics, as AI is programmed to analyse and process huge data sets and come to conclusions based on them quickly which may help the military commander on the battlefield to make algorithm and data-based decisions. Automation and Optimization is also a benefit of AI-oriented cyber operations as it results in reduced manual efforts and increased efficiency, leading to operational excellence in cyberspace.

Therefore, AI’s applicability in the context of cyberspace, just like any other technological innovation, has definitely transformed cybersecurity norms by laying out more modernised technologies to detect, prevent and protect from cyber threats or attacks. AI- oriented cyberoperations make is easier to analyse huge sets of data and have quick responses to the situations of threat on the battlefield. AI has also

revolutionised routine security tasks such as monitoring and surveillance leading to reduction of human error and workforce. However, AI-oriented systems are not unerring as they may generate false negatives, false targeting and damaging civilian objectives as a consequence of cyber threat detections. Arriving at an optimum balance between sensitivity and specificity requires a lot of research and data for the purposes of appropriate analysis. Hence, integrating AI on the battlefield specially requires a complex infrastructure, skill set and financial resources.

II. CRIMINAL LIABILITY FOR AI-ORIENTED CYBER OPERATIONS UNDER INTERNATIONAL CRIMINAL LAW

The recent two decades to be precise, have witnessed the growing use of cyber technologies on the battlefield including spreading of false information, data theft, breach of government computers and machineries, stealing state secrets, etc. It is important to understand that the use of such technology is increasing day by day as the States are developing and utilizing cyber-weaponry as a means and method of warfare and also, using AI-oriented systems to operate such cyber weapons. Therefore, the conduct of hostilities is not limited to cyber weaponry but the such weaponry being run by AI-oriented systems on the behalf of military commanders in the times of war. Such cyber operations are often combined with the traditional means and method of warfare, resulting in a “blended attack”.

The State actors tend to develop such cyber-technology with utmost carefulness in order to adhere to the rules and principles of IHL i.e., which are able to differentiate between the military and civilian objectives, limit the scope of collateral damage, proportional to the military objectives sought to be achieved and so on. Yet, in the cases of cyber operations which are AI- oriented and run by such systems based on algorithms and huge databases, the chances of violation of IHL are prominent but the accountability gap exists and the question of command responsibility arises i.e., whether the military commander who was in-charge of such operations liable for the consequences of such violations. There are extreme chances that such cyber operation may proliferate beyond their set targets and be “repurposed” for attaining ulterior motives. In such cases, ICL demands that the perpetrators should be well punished and held accountable for their actions. But can a software or a system which is AI-oriented be held responsible? Does such software or system qualify the “mental element” requirement under the rules of ICL? Such questions create a lot of confusion and dilute the purposes of law.

The concept of Autonomous Weapon System (AWS) basically means such military technologies that are

self-instructing i.e., capable of operating by themselves without any direct human intervention as they are run by AI, based on algorithms and huge databases. While such systems have the potential to enhance military capacities, their development needs conscious care with regard to the rules and regulations of IHL i.e., the principles of humanity, distinction, military necessity and proportionality. In such cases, wherein there is no human intervention with the AWS, there are high chances of such consequences which may harm the civilians or target civilian objectives resulting in the violation of IHL. Another prospect includes the scenarios wherein “automation bias” may occur and the military man follows the AI’s suggestions based on data inbuilt in the system and acts without the application of his own mind i.e., reasonable military man’s mindset. These above notions are a topic of ongoing debate under the laws of armed conflict, leading to the need for additional norms and regulations.

With regard to ICL, there are two types of international crimes that can arise from the application of AI on the battlefield. Firstly, war crimes i.e., grave violations of the core rules and principles of IHL, like online assaults of civilians, use of such weapons which are prohibited under IHL, targeting civilian objectives with the help of drones, etc. And secondly, crimes against humanity, which may include the use of AI for unauthorised civilian surveillance or mass arrests.

But with regard to who should be held liable for such crimes, it is essential to comprehend AWS and the “criminal liability gap” that persists in the realm of ICL. This gap can be viewed from various perspectives, one being that humans should be held liable for any acts of AWS, whether they are legal or illegal. This approach deals with AWS as product of human creation and cannot exceed beyond the database that is inbuilt in it by human creators. Another perspective covers those researchers who contend that AWS’s autonomy creates a certain level of instability, unpredictability and zero to low jurisdiction by humans, therefore, leaving humans of any liability in case of any violations. The Author here argues that the third approach, i.e., the utilitarian approach should be considered as the appropriate which assigns collective responsibility to all the stakeholders involved but at the same time downplays the notions of individual criminal responsibility and relies entirely on state liability.

Here, the concept of autonomy can be viewed from two perspectives i.e., wherein the military commander only supervises (the man in the loop) and wherein he has no participation at all (the man out of the loop). Considering this, the International Criminal Tribunal for the Former Yugoslavia (herein, referred to as

ICTY) specified that “the accused needs criminal intent by way of knowledge that the accomplice’s action with assist the perpetrator in the commission of the crime.” Further, the ICTY has also specified that “the requisite actus reus would be effective control i.e., the ability to prevent and punish the commission of such war crimes.” Such understanding gives rise to the notion that state liability is a correct model which is traditionally more compliant with ICL and also helps the military to use such advanced AWS systems rather than discarding them due to the problems of human accountability. But in order to align with the realm of IHL, Article 43 of the Additional Protocol I to the Geneva Conventions, specifies that states are only accountable for illegal actions performed by their military personnels, meaning that no offence committed by AWS would result in direct state liability. Therefore, there should be bent towards individual criminal liability on the battlefield. As stated well by Sparrow, “it is a fundamental condition of fighting a just war that someone may be held responsible for the deaths of enemies killed in the course of it.” Therefore, in case of any war crime perpetrated by AWS or LAWS, there should be assignment of criminal liability at both the State and individual level.

III. WAR CRIMES AND GRAVE BREACHES IN AI-ORIENTED CYBER OPERATIONS

Currently, there are numerous ways of applying AI in the context of military and on the battlefield. They include Assisted decision-making systems for the purposes of targeting military objectives, particularly the use of lethal autonomous weapons systems (hereinafter, referred to as LAWS), leading to two major questions of how are dealt under the exigencies of IHL and ICL simultaneously and another censorious notion of attribution of responsibility for any actions taken by such systems on the battlefield or any resultant violations if IHL in this regard.

At this point of discussion, it is important to recognize that neither AWS nor LAWS are just simple machines but to state simply, sociotechnical systems which involve both machinery components and human intellect i.e., software developers, manufacturers, engineers, operators and users which leads to the conclusion that the “responsibility gap” is in the hands of multiple stakeholders.

Some authors suggest for a “blank check liability” wherein the humans hold themselves accountable and liable for any act on the behalf of the AI, whereas other group of authors propose a strict criminal liability in criminal law for such violations of IHL by AI-oriented systems. Some scholars also argue against the notions of direct individual criminal liability for operators (in this case, the military commanders) in context of AWS or LAWS, stressing on the fact that

such liability requires intention or failure to apply reasonable mind resulting in recklessness leading to a concrete instrumental connection between the action and outcome. This view point works on the premise that the attacks by AWS or LAWS lack guilty mind of the military commander as there is limited human control, and hence, direct individual liability cannot be established.

However, answer to the above confusion is rooted in the concept of “Command Responsibility” which makes military commanders criminally responsible for any war crimes perpetrated by their subordinates. This article holds this form of liability as appropriate to hold the military commanders responsible for any act done by his subordinates, be it AWS or LAWS and establishes a causal link of supervision between the two. This jurisprudential doctrine tends to hold the military commander responsible if “they have actual control over a subordinate’s criminal actions, know or have any reason to know of such actions, and fail to take necessary and reasonable measures to prevent or punish them.” The author argues here that in such cases the situation of the military commander represents that of an agent who is deciding under risk and that he should have been well aware of any future consequences of an act by AWS or LAWS. He cannot negate his responsibility by stating that such an AI-oriented system was not in his “control” and acted according to its own whims and fancies.

Countering the authors above argument, some authors are also of the viewpoint that holding the military commanders responsible for such acts of the AWS or LAWS is unreasonable and making them liable purely on descriptive factors is incorrect. However, this is not the part of discussion in this article.

CONCLUSION AND SUGGESTIONS

By an in-depth analysis of AI in the cyberspace, this research paper endeavours to contribute to the ongoing discussions around the need for a technologically advanced and updated legal regime. One of the most important arguments against the use of AWS or LAWS is the notion that it will lead to “responsibility gap” on the battlefield as the State may not hold any responsibility for such actions and at the same time, the distance between autonomy and commands of the military commander grows extensively. Hence, it becomes even tougher to hold any one individual responsible for such crimes, leading to the growing of “responsibility gap”.

It is need of the hour to understand that the concept of command responsibility in the case of AI-oriented systems i.e., AWS and LAWS fails to follows the exigencies of subordinate-superior relationship as the individual behaviour of such autonomous systems disturbs the chain of command which exists between

the military commander and the system, as he has no effective control over such systems because they obtain, process and decide on a large number of information from their databases and function on algorithms. Therefore, the speed of military commander or a human controller cannot match with such technologically advanced systems. As a result, the traditional notion of command responsibility does not fit in with such advancements.

The author highlights that striking a right balance between technological advancements and regulation is the key. The current concepts of command responsibility and individual criminal responsibility should be modernised in order to hold the military commander effectively responsible for any violations or war crimes committed on the battlefield under the regime of IHL and ICL.

Ideally the military commander should be held responsible regardless of the fact that the machines performed unexpectedly or as an unforeseeable consequence of the use of automated machines or systems happened. This responsibility includes criminal liability as well as administrative accountability, in which the commander bears personal liability for the weapons unleashed on the battlefield and as subject to the sanctions for violations of IHL. Hence, the author in this research paper vouches that the traditional concept of command responsibility does not align with the modern-day weaponry and therefore, there is a need for amendments in this regard.

BIBLIOGRAPHY

1. Bellovin S, 'Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications' (2017) 3 *Journal of Cybersecurity* 59
2. Bhusan T, 'Artificial Intelligence, Cyberspace and International Law' (2024) 21 *Indonesian J Int'L* 281, 284
3. Boutin B, 'Legal Question Related to the Use of Autonomous Weapon System' (2021) *Asser Institute*
4. Champagne M, 'Bridging the Responsibility Gap in Automated Warfare' (2013) 28 *Philosophy & Technology* 125, 128
- 5.
6. Crootof R, 'War Torts: Accountability for Autonomous Weapons' (2016) 164 *University of Pennsylvania Law Review* 1347
7. Edward L and Veale M, 'Slave to the Algorithm? Why a 'Right to an Explanation' is Probably not the Remedy you are looking for' (2019) 16 *Duke Law and technology Review* 22
8. Guenael M, 'The Law of Command Responsibility and the Principle of Legality' (2009) *Oxford Law Pro* < /academic.oup.com/oxford-law-pro/book/43011> accessed 17 January 2026
9. Hammond D, 'Autonomous Weapons and the Problem of State Accountability' (2014) 15 *Chicago Journal of International Law* 652
10. Kraska J, 'Command Accountability for AI Weapon Systems in the Law of Armed Conflict' (2021) 97 *Int'l L Stud Ser US Naval War Col* 407
11. Macak K, 'Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors' (2016) 21 *Oxford University Press* 405
12. Makalesi A, 'Command Accountability for AI Weapon Systems in the Laws of Armed Conflict' (2023) 10 *Asbider* 111, 113
13. Marguiles P, 'Making Autonomous Weapons Accountable: Command Responsibility for Computer-Guided Lethal Force in Armed Conflicts' in Jens David Ohlin, *Research Handbook on Remote Warfare* (Edward Elgar Publishing 2017)
14. Marra B and McNeil S, 'Understanding "The Loop": Regulating the Next Generation of War Machines' (2013) 36 *Harvard Journal of Law & Public Policy* 1140, 1153
15. Oimann A and Salatino, 'Command Responsibility in Military AI Contexts: Balancing Theory and Practicality' (2024) *AI and Ethics* 1757
16. Shehata M, 'The Impact of Artificial Intelligence in Military Operations in the Light of International Humanitarian Law' (2024) 4 *Journal of Law and Emerging Technology* 13, 37
17. Slidregt E, 'Command Responsibility and Cyberattacks' (2016) 21 *J Conflict & Sec L* 505
18. Trahan J, 'The Criminalization of Cyber-Operations Under the Rome Statute' (2021) 19 *Journal of International Criminal Justice* 1133, 1148
19. Vallor S and Vierkant T, 'Find the Gap: AI, Responsible Agency and Vulnerability' (2024) 34 *Mind and Machines* 20