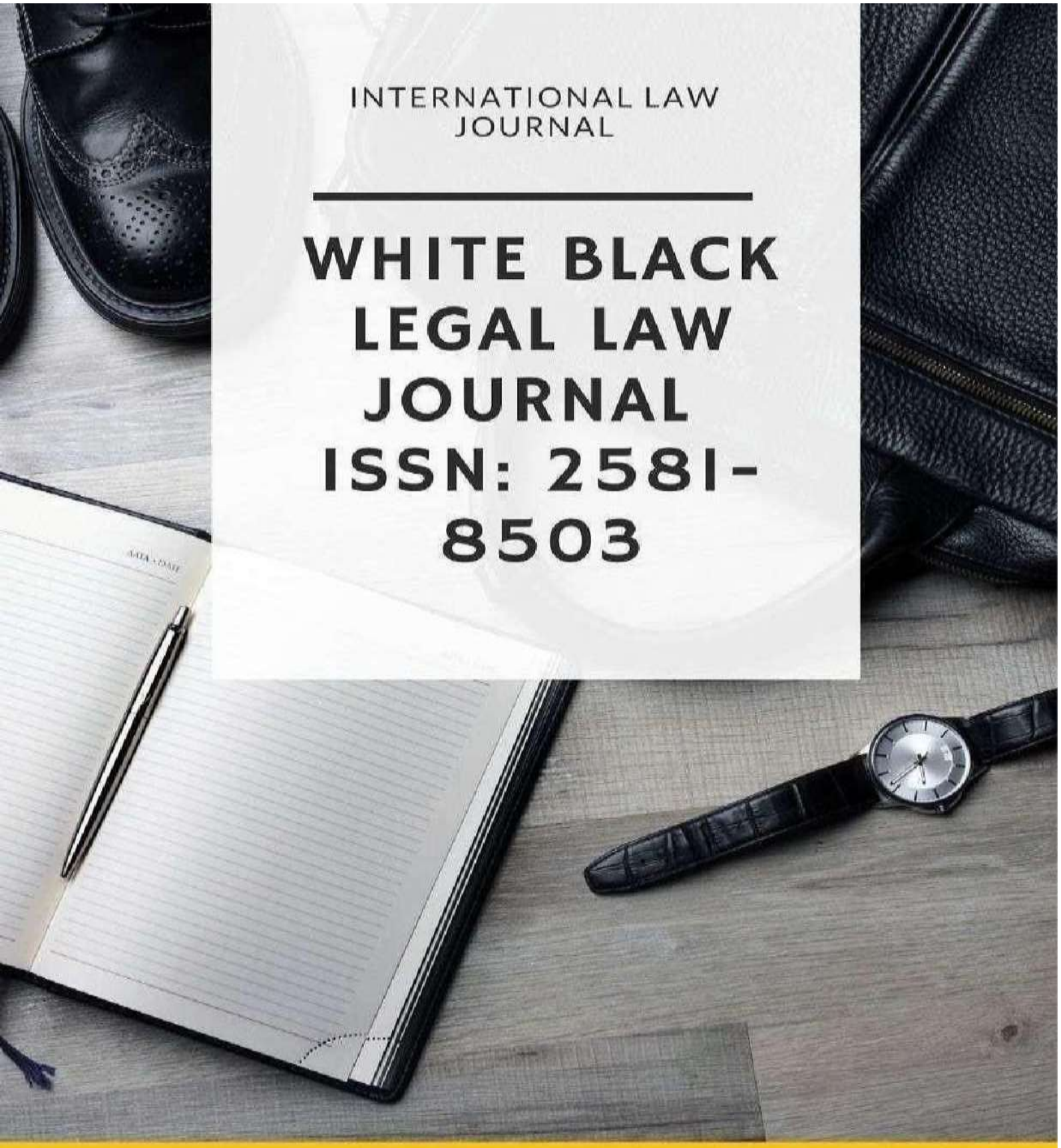

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in ‘Intercountry adoption laws from Uttranchal University, Dehradun’ and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and

refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | Dec 2024 ISSN: 2581-8503

ACCOUNTABILITY IN THE AGE OF MACHINES: CRIMINAL RESPONSIBILITY FOR AUTONOMOUS WEAPON SYSTEMS

AUTHORED BY - VISHNU PRIYA KOLLI

ABSTRACT

This research makes a significant contribution to the ongoing debate surrounding autonomous weapon systems (AWS) and the issue of accountability. It provides valuable insights for a wide range of stakeholders, including policymakers, legal scholars, technologists, and military professionals, all of whom are grappling with the ethical and legal implications of AWS. By exploring and addressing the gaps in accountability, particularly in scenarios where AWS may cause unintended harm, this study seeks to promote responsible innovation in the development and deployment of these technologies.

Furthermore, it emphasizes the importance of ensuring that AWS complies with international humanitarian and human rights law, thereby safeguarding human dignity in the context of warfare and security. By offering a nuanced understanding of the responsibility involved in AWS use, this paper argues that accountability should ultimately rest with the individuals and entities involved in the deployment and operational control of these systems. In doing so, it seeks to establish clear legal and ethical guidelines to prevent impunity and ensure that the deployment of AWS aligns with broader societal values, including the protection of life and the upholding of international norms.

This paper delves into the intricate issue of criminal responsibility in the context of AWS, exploring how the increasing autonomy of these systems intersects with existing legal principles. By thoroughly analyzing current legal frameworks, relevant case studies, and expert opinions, the research seeks to clarify the concept of autonomy in weapon systems and its impact on criminal responsibility. The paper also examines the accountability gaps that exist within the current international legal regime, highlighting how these gaps create challenges in ensuring that those responsible for AWS-related violations of international law can be identified and held accountable.

INTRODUCTION

The development and deployment of Autonomous Weapon Systems (AWS) have significantly transformed modern warfare, introducing new challenges and reshaping the battlefield in unprecedented ways. As machines increasingly take on roles traditionally reserved for human soldiers, including making critical life-or-death decisions, fundamental questions arise about accountability and criminal responsibility. These autonomous systems, equipped with advanced algorithms and artificial intelligence, challenge the established norms of international humanitarian law (IHL) and criminal justice, which have historically been centered on human actors and their decision-making processes.[1]

One of the most pressing concerns is the lack of clarity on who bears responsibility for violations of international law when AWS is involved. This ambiguity represents a serious threat to global security, human rights, and the rule of law, as the introduction of AWS complicates the attribution of responsibility in cases of unlawful harm or destruction. Given that AWS, often referred to as "killer robots," can operate independently without direct human oversight, the question of accountability becomes even more critical. These systems can select, engage, and potentially kill targets based on pre-programmed parameters and real-time data analysis, all without a human directly in the decision loop.[2]

This raises several urgent and complex questions: Who should be held accountable for the harm caused by AWS on the battlefield? Is it the programmer who designed the system, the military commander who authorized its deployment, the manufacturer who built the hardware, or the state that sanctioned its use? The current legal frameworks do not offer a clear answer, and this ambiguity undermines international efforts to prevent and prosecute war crimes. The lack of clear attribution of responsibility could embolden actors to deploy AWS with less regard for the legal and ethical consequences, increasing the risk of violations of international humanitarian law.[3]

This research proposes potential solutions to address these accountability gaps. It explores the role of various actors—states, manufacturers, programmers, and individuals—in ensuring

[1]Dan Saxon (Ed.), International Humanitarian Law and the Changing Technology of War (2020).
[2] Robert Sparrow, Killer Robots: The Future of War? (Routledge 2017).
[3] James Crawford, Responsibility of States and Individuals in International Law, Oxford International Law Library (Oxford University Press 2014).

compliance with international law and preventing unlawful use of AWS. The paper argues for the development of new legal frameworks or the adaptation of existing ones to explicitly address the unique challenges posed by autonomous weapon systems. It also calls for stronger mechanisms to ensure oversight, transparency, and accountability in the development, deployment, and use of AWS in order to safeguard human rights, uphold international humanitarian law, and maintain the rule of law in an increasingly automated and technologically advanced world.

RESEARCH QUESTIONS

Through this study, the following questions will be analyzed to understand the criminal responsibility of AWS system deployment: -

1. Who bears criminal responsibility for AWS-related violations of international law?
2. How do existing legal frameworks address accountability for AWS?
3. What reforms or new frameworks are necessary to ensure accountability and prevent impunity?

METHODOLOGY

This research will adopt a mixed-methods approach, integrating multiple methodologies to provide a comprehensive and well-rounded analysis of the legal and ethical implications of Autonomous Weapon Systems (AWS). By critically examining existing treaties, conventions, and legal principles, the research will evaluate the extent to which these legal doctrines address the accountability challenges posed by autonomous weapon systems. The doctrinal analysis will form the backbone of the research, helping to identify gaps and ambiguities in the current legal frameworks that may leave room for impunity when AWS-related violations occur. The research will include detailed case studies of real-world AWS development and deployment.

These case studies will examine specific instances where autonomous weapon systems have been used in military operations, focusing on the legal, ethical, and practical challenges that have emerged. By analyzing both successful and controversial uses of AWS, the research aims to identify patterns in how these systems are developed, tested, and deployed, as well as how responsibility is attributed in practice. This mixed-methods approach aims to provide a holistic understanding of the accountability challenges posed by autonomous weapon systems. This approach will enable the research to not only critique existing legal frameworks but also

propose practical, forward-thinking solutions that reflect the complexities of modern warfare and technology.

AWS: DEFINITION AND DEVELOPMENT

Autonomous Weapon Systems (AWS) are advanced military technologies capable of selecting, engaging, and destroying targets without the need for direct human intervention. These systems rely on a combination of sophisticated sensors, artificial intelligence (AI), and machine learning algorithms to detect, identify, and respond to potential threats in real time.[4] Once deployed, AWS can operate independently, meaning they have the capacity to make decisions on the battlefield without ongoing human oversight or input. These systems are programmed to analyze data, process environmental conditions, and assess threats based on pre-defined criteria, allowing them to initiate attacks autonomously, even without receiving a direct command from a human operator. AWS are capable of selecting targets based on factors like movement patterns, heat signatures, or other predefined behavioral indicators, making decisions based on the parameters set by their developers and military operators.[5]

Ultimately, these systems are designed with the specific intent to cause harm or destruction, fulfilling their role as combat technologies within military operations. However, the development and deployment of AWS are accompanied by several significant challenges that need to be addressed before these systems can be safely and ethically integrated into modern warfare. One of the foremost challenges in AWS development is ensuring the reliability and accuracy of these systems. AWS rely on AI and machine learning algorithms to assess complex battlefield environments, which are often unpredictable and chaotic. If the systems misinterpret data or make incorrect decisions, there is a risk of targeting civilians, friendly forces, or neutral actors, leading to unintended casualties or destruction. Ensuring that AWS can accurately differentiate between combatants and non-combatants, as well as between legitimate military targets and civilian infrastructure, is a critical concern that requires ongoing technological refinement.[6]

[4] Nathan Leys, Autonomous Weapon Systems and International Crises, Strategic Studies Quarterly, Vol. 12, No. 1 (SPRING 2018), pp. 48-73 (26 pages).
[5] U.N. Office for Disarmament Affairs, Autonomous Weapons Systems: Technical, Military, and Legal Aspects (2017).
[6] Benjamin Wittes, The Future of Violence: Robots and Drones, Cyberwar, and Cybersecurity (Brookings Institution Press 2015).

As with any system dependent on advanced software and networked technologies, AWS are vulnerable to cyberattacks. Hackers or adversaries could potentially compromise the system's decision-making algorithms or manipulate the data being processed by AWS, leading to catastrophic outcomes. A compromised AWS could be used to target unintended locations or engage in unintended combat operations. Ensuring robust cybersecurity protections for AWS is essential to prevent unauthorized access, hacking, or data manipulation, which could undermine the security of entire military operations.

The use of AWS raises profound ethical questions, particularly around the delegation of life-or-death decision-making to machines. When AWS independently selects and engages targets, human operators are removed from the immediate decision loop, which raises concerns about accountability for actions taken by these systems. If AWS were to violate international humanitarian law by attacking civilians or committing war crimes, it is unclear who would be held responsible—the programmer, the commander, the manufacturer, or the system itself.[7] These ethical dilemmas are central to the ongoing debates surrounding the legality and moral acceptability of AWS, highlighting the need for clearer frameworks for accountability.

Existing regulatory frameworks and international legal standards, including international humanitarian law (IHL) and international human rights law (IHRL), were established with human actors in mind and may not be fully equipped to regulate the use of autonomous systems. As AWS operate without human oversight, current laws may not adequately address the unique challenges of ensuring compliance with the laws of war, such as proportionality and distinction.[8] The lack of a clear and binding international framework for the use and control of AWS presents a significant regulatory challenge as nations grapple with how to regulate and restrict the use of these systems in a manner consistent with international law.

Addressing these development challenges is critical to ensuring that AWS can be deployed responsibly and ethically, with appropriate safeguards in place to prevent harm to civilians, protect human rights, and uphold the rule of law on the battlefield. Advances in technology, coupled with the development of robust legal and regulatory frameworks, are essential to

[7] Autonomous Weapon Systems and International Humanitarian Law, Journal of International Law, 381-405 (2018).
[8] J.D. Ohlin, '*The Combatant's Stance: Autonomous Weapons on the Battlefield'*, International Law Studies (2016), at 9–10, 21.

mitigating the risks associated with AWS and ensuring that their use is consistent with the principles of international law.

Current Examples:

1. US: Lockheed Martin's Long Range Anti-Ship Missile (LRASM)
2. Russia: Uran-9 Unmanned Ground Combat Vehicle
3. Israel: Iron Dome Air Defense System
4. China: Sharp Sword Unmanned Combat Air Vehicle

LEGAL FRAMEWORKS

These provisions address foundational principles such as the distinction between combatants and non-combatants, proportionality in attacks, and precautions during military operations. They are critical for determining whether AWS can be deployed in a manner that complies with international legal norms and, importantly, who bears criminal responsibility in cases where AWS causes violations of these laws. Article 48 of Additional Protocol I (AP I) to the Geneva Conventions establishes the principle of distinction, which requires that parties to a conflict differentiate between combatants and non-combatants, as well as between military objectives and civilian objects.[9] AWS, which operates autonomously and makes decisions based on pre-programmed algorithms, must adhere to this principle in real-time battlefield scenarios. If an AWS fails to properly distinguish between civilians and legitimate military targets and causes harm to non-combatants, a violation of IHL could occur.

Article 51 of AP I sets forth the principle of proportionality, which prohibits attacks that would cause excessive harm to civilians or civilian objects in relation to the anticipated military advantage. AWS, when executing autonomous attacks, must balance the need to neutralize a military target with the risk of collateral damage to civilian populations or infrastructure.[10]

Article 57 of AP I requires that all feasible precautions be taken in planning and executing military operations to minimize harm to civilians and civilian objects.[11]AWS must be designed

[9] Art. 48, International Committee of the Red Cross (ICRC), Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention), 75 UNTS 287, 12 August 1949.
[10] Art. 51, International Committee of the Red Cross (ICRC), Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention), 75 UNTS 287, 12 August 1949.
[11] Art. 57, International Committee of the Red Cross (ICRC), Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention), 75 UNTS 287, 12 August 1949.

to incorporate these precautions into their decision-making processes, ensuring that civilian harm is avoided or minimized wherever possible. This provision is crucial when considering the autonomy of AWS, as these systems must be programmed to assess and react to rapidly changing battlefield conditions in a manner consistent with IHL.

The CCW was established to restrict or ban the use of certain types of weapons that are considered excessively injurious or have indiscriminate effects. The CCW emphasizes that states or entities that use such weapons must ensure their use complies with IHL, particularly in minimizing harm to civilians and avoiding unnecessary suffering.[12]

The CCW reinforces the principle that the state or actor responsible for **deploying** a weapon system must ensure its use aligns with international law. By analogy, this can be extended to AWS. If AWS are deployed in a way that leads to unlawful harm—whether through indiscriminate attacks or excessive collateral damage—the **responsibility** would lie with the party that deployed the system. Just as with conventional weapons, the legal and moral duty to ensure that AWS do not violate IHL rests with those who control and deploy them. In this sense, the CCW provides a foundation for arguing that the decision to deploy AWS carries with it an obligation to prevent violations of international law, making the deploying entity accountable for any breaches.

Protocol III of the CCW imposes restrictions on the use of incendiary weapons, particularly in civilian areas, due to their devastating and indiscriminate effects. It mandates that the parties deploying such weapons must take precautions to avoid unnecessary harm to civilians and civilian objects.[13]

The restrictions in Protocol III highlight the responsibility of the party **deploying** a weapon to ensure it is used in a manner that complies with IHL. By deploying AWS, the actor similarly assumes responsibility for the system's actions. If an AWS, for instance, causes indiscriminate harm or fails to differentiate between military and civilian targets, the **responsibility for the violation** falls on the entity that authorized its deployment. This aligns with the paper's argument that the act of deploying an AWS entails direct accountability for any legal violations

[12] Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons, 21 December 2001.
[13] Protocol III, Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons, 21 December 2001.

the system may commit, as the entity in control of the deployment must ensure the system operates within the constraints of IHL, just as they must with incendiary weapons under Protocol III.

The legal obligations set out in Protocol IV demonstrate that **responsibility for unlawful outcomes** falls on the party that decides to deploy the prohibited weapon. This principle can be extended to AWS, which—if deployed recklessly or without proper safeguards—could result in violations of international law similar to those committed by blinding laser weapons.[14]

The entity deploying AWS must ensure that the system complies with IHL's core principles, such as distinction and proportionality. If AWS are used in a manner that violates these principles, **criminal responsibility** should rest with those who deployed them, as is the case with blinding laser weapons under Protocol IV. The decision to deploy such a system includes the responsibility to ensure that its actions are lawful, making the deploying entity accountable for any resulting breaches.[15]

ACCOUNTABILITY GAPS

There are key accountability gaps and challenges in establishing **criminal responsibility** for **Autonomous Weapon Systems (AWS)**, which complicate efforts to ensure compliance with international law and prevent impunity.

One of the primary challenges in AWS accountability is the uncertainty over **who is responsible** when these systems violate international humanitarian law (IHL). Since AWS can operate independently and make decisions autonomously, it is unclear whether criminal responsibility should lie with the military commander who deployed the system, the programmer who developed its algorithms, or the manufacturer who created the technology. The lack of clear legal precedents or guidelines on AWS accountability creates ambiguity in assigning responsibility, making it difficult to hold any individual or entity accountable when these systems cause harm.[16]

[14] Protocol IV, Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons, 21 December 2001.
[15] Bhuta, Nehal et al., *Autonomous Weapons Systems: Law, Ethics, Policy* (2016).
[16] Roger S Clark, '*The Mental Element in International Criminal Law: The Rome Statute of the International Criminal Court and the Elements of Offences'* (2001) 217 Criminal Law Forum.

AWS relies on complex algorithms and machine learning processes to make decisions, which often operate in a "black box" manner, meaning that the decision-making process is not transparent or easily traceable. This creates a major challenge in understanding **how and why certain decisions were made**, such as selecting a target or initiating an attack. Without the ability to trace the decision-making process, it becomes extremely difficult to identify if any violations occurred and, more importantly, to determine who is responsible for those violations. This lack of transparency complicates efforts to hold individuals or entities accountable for AWS-related actions.

A fundamental challenge in establishing **criminal responsibility** in international law is proving intent. In cases involving AWS, it is difficult to prove the necessary intent to commit war crimes or other violations, as autonomous systems lack human intent or motive. Since AWS decisions are driven by algorithms and pre-programmed instructions, there may be no clear evidence of malicious intent behind harmful actions.[17] This complicates the legal process of attributing criminal responsibility, as intent is a key element in prosecuting war crimes and violations of IHL.

Under international law, states are responsible for ensuring that the weapons they develop and deploy comply with international humanitarian law. However, in the case of AWS, where the system operates independently of direct human control, it is unclear to what extent states can be held accountable for violations committed by these systems. This uncertainty presents a major challenge for international law, as states may attempt to distance themselves from the actions of AWS, arguing that they had no direct control over the system's decisions. This complicates efforts to hold states responsible for ensuring that AWS use is lawful and in line with international obligations.

This paper argues that criminal responsibility for the actions of Autonomous Weapon Systems (AWS) should rest with the individuals or entities that deploy these systems. To illustrate this point, we will examine the use of autonomous systems in three contexts beginning with by the U.S. military, which has increasingly integrated such technologies into its operations, raising significant questions about accountability and oversight.

[17] MOHAMED ELEWA BADAR, '*The Mental Element in the Rome Statute Of The International Criminal Court: A Commentary from A Comparative Criminal Law Perspective'* (2008) 19 Criminal Law Forum 473, 475.

1. **U.S.'s UAVs**

The U.S. military has made substantial investments in various autonomous systems, including unmanned aerial vehicles (UAVs), unmanned ground vehicles (UGVs), and autonomous underwater vehicles (AUVs). For example, the Lockheed Martin Long Range Anti-Ship Missile (LRASM) is a notable AWS with lethal capabilities designed to operate with a high degree of autonomy.[18] The U.S. military has conducted operational testing of these systems across diverse environments, aiming to enhance combat effectiveness while minimizing risk to personnel. However, the deployment of such systems has led to critical questions regarding accountability for harm caused by their operations. In situations where AWS are involved in actions that result in civilian casualties or violations of international humanitarian law, determining who is liable becomes crucial. The **principle of command responsibility**—which holds military commanders accountable for the actions of their subordinates—plays a pivotal role in this context. Commanders are expected to exercise control and oversight over their units, including the systems they deploy, making them potentially liable for violations committed by those systems.[19]

DoD's Autonomous Systems policy emphasizes the importance of ensuring that all autonomous systems operate within legal and ethical boundaries. It stipulates that the Department of Defense (DoD) will maintain a human-in-the-loop approach to critical decisions, thus placing responsibility for decisions squarely on the shoulders of human commanders and operators. The doctrine of unmanned systems establishes guidelines for the operational use of unmanned systems, highlighting the need for robust command and control processes. It reinforces the idea that commanders must remain accountable for the actions of unmanned systems under their control, particularly in terms of adhering to international laws governing armed conflict.[20]

The U.S. Air Force's Autonomous Systems strategy of 2019 outlines the Air Force's vision for integrating autonomous systems while ensuring compliance with ethical standards and accountability. It emphasizes the necessity of maintaining human oversight over autonomous operations and the responsibility of commanders to mitigate risks associated with AWS.

[18] US - UAV
[19] National Academy of Science, Eng., & Med., *Autonomous Vehicles: Status, Challenges, and Opportunities* for Smart Growth, 11-36 (2019).
[20] *Id.*

By focusing on the chain of command and decision-making processes within the U.S. military, this paper argues that commanders must be held accountable for the actions of the AWS they deploy. This accountability framework not only reinforces the principles of international humanitarian law but also serves as a deterrent against reckless or unlawful use of autonomous technologies.

2. IRON DOME: A CASE STUDY IN AUTONOMOUS WEAPON SYSTEMS

The Iron Dome is a sophisticated air defense system designed to intercept and destroy incoming rockets, artillery shells, and mortar bombs. It operates through a combination of radar and advanced computer algorithms that autonomously detect and track threats. Once a rocket is identified, the Iron Dome's algorithm determines whether to engage the threat based on a series of programmed criteria, often without any human intervention.[21] While the system has proven effective in protecting civilian populations from missile attacks, its use raises crucial questions about the accountability for civilian casualties that may result from its operations.

One of the central issues concerning the Iron Dome is the question of **who bears responsibility for civilian casualties** that occur as a result of its interceptions. When Iron Dome interceptors engage a target, they must make rapid decisions that can have life-or-death consequences. If a missile is intercepted in a populated area, the resulting explosion could harm civilians. The commanders who authorize the deployment of Iron Dome systems must ensure compliance with international humanitarian law (IHL) principles, including distinction and proportionality. If the system causes civilian casualties, these commanders could be held accountable for failing to implement appropriate operational procedures or for choosing to deploy the system in an area with high civilian presence.[22] The state that deploys the Iron Dome system also bears responsibility for ensuring that its military operations comply with international legal standards. If the use of Iron Dome results in violations of IHL, the state could face legal and diplomatic repercussions, including accusations of war crimes.

The command responsibility framework must be rigorously applied to the deployment of AWS, ensuring that human actors retain responsibility for the systems

[21] Rizky Citra, *A Defense for Guardian Robots: Are Defensive Autonomous Weapons Systems Justifiable?*, Harvard Law Journal, 8 February 2024.
[22] *Id.*

they utilize in conflict situations. This approach is critical for maintaining the rule of law and protecting civilian lives in an increasingly automated battlefield.

3. RUSSIA'S URAN-9 UNMANNED GROUND

The Uran-9 is an advanced robotic vehicle designed for combat operations, equipped with autonomous features that allow it to navigate pre-programmed paths and engage targets without direct human intervention. While the technology represents a significant advancement in military capabilities, it also highlights the urgent need for clear accountability guidelines. The complexities surrounding the Uran-9's autonomous functions necessitate a thorough examination of who bears responsibility for its decisions, especially in contexts where these decisions could result in harm to civilians.[23]

The Uran-9 has been deployed in conflict zones such as Syria, where its operational use raises pressing accountability concerns. Military commanders play a crucial role in overseeing the deployment and operation of the Uran-9. Command responsibility entails the obligation of commanders to ensure that their subordinates adhere to established rules of engagement and comply with international humanitarian law (IHL). In the case of the Uran-9, commanders must ensure that the vehicle operates within the confines of these legal frameworks. If the vehicle engages a target that results in civilian casualties, the chain of command should be scrutinized to determine whether the commanders fulfilled their responsibilities in preventing such outcomes. Another critical concern is the potential for unauthorized or malfunctioning vehicles to cause harm. Commanders must implement robust safety protocols and operational checks to prevent the Uran-9 from acting outside its designated parameters. This includes measures to ensure that the vehicle cannot initiate attacks autonomously without appropriate oversight, thereby mitigating the risk of accidental engagements. The increasing autonomy of systems like the Uran-9 challenges the assumption that human oversight is a given in military operations. As these systems operate independently, the need for clear accountability becomes paramount. If the Uran-9 makes a decision that leads to civilian harm, the question arises: who is responsible? As these technologies continue to evolve and become integrated into military

[23] Dr. Marta Bo, Three Individual Criminal Responsibility Gaps with Autonomous Weapon Systems, 29 November 2022.

operations, establishing clear guidelines for accountability will be vital to prevent unnecessary harm and uphold the principles of international humanitarian law. By emphasizing the role of command responsibility, this paper underscores the need for military commanders to retain accountability for the actions of autonomous systems, ensuring that ethical and legal standards are upheld in the increasingly automated landscape of modern warfare.

POSSIBLE SOLUTIONS

While AWS is designed to operate autonomously, there must be **clear limits on their autonomy** to prevent unintended harm, particularly in situations where complex ethical and legal judgments are required. AWS should not be granted full autonomy in decisions involving the use of lethal force, as the risks of unlawful harm increase in the absence of human judgment. Limiting the degree of autonomy granted to AWS would involve setting constraints on their ability to select targets, initiate attacks, or make other critical decisions without human input.[24] One of the central challenges in holding individuals or entities accountable for AWS-related violations is the lack of a clear **chain of command** and decision-making process when AWS is deployed.

To protect civilians from the potential harms associated with AWS, the establishment of **AWS-free zones** could be a proactive measure. These zones, similar to nuclear-weapon-free zones, would prohibit the use or deployment of AWS in areas where civilians are present, such as densely populated urban centers or civilian infrastructure. Creating these zones would provide an additional layer of protection for civilians, reducing the risk of accidental or indiscriminate harm caused by AWS.[25] These zones would also provide a safeguard against the risks of AWS malfunction or misuse, ensuring that the most vulnerable populations are shielded from the dangers of autonomous warfare technologies.

AWS operate with a level of autonomy that removes direct human involvement in decision-making, leading to ambiguity about who is responsible for the system's actions. To address this, it is essential to establish explicit chains of command that clearly identify the individuals responsible for the decision to deploy AWS, monitor their actions, and ensure compliance with

[24] International Committee of the Red Cross, *Autonomous Weapon Systems and the Law: The Human Role*, ICRC Law & Policy Blog (Nov. 11, 2021).
[25] *Id.*

legal standards. To ensure accountability for AWS-related actions, it is critical to develop **comprehensive national and international regulations** governing their development, deployment, and use. Currently, there are significant gaps in the legal frameworks that regulate AWS, both at the national and international levels.

No single state or legal system can effectively regulate AWS on its own, as these technologies often have cross-border implications. International forums, such as the United Nations or other multilateral organizations, can play a vital role in facilitating dialogue among states to develop common standards for AWS use. While AWS are designed to operate autonomously, human involvement remains crucial to prevent unintended or unlawful harm. Introducing human oversight mechanisms would involve having human operators or commanders review and approve the critical decisions made by AWS, particularly those related to the use of force.

To ensure that AWS-related violations of international law do not go unpunished, it is crucial to hold **commanders accountable** for the harm caused by the systems they deploy. Military commanders and decision-makers bear ultimate responsibility for the actions of the weapon systems under their control, including AWS. This means that commanders should be held criminally or legally liable if AWS cause unlawful harm, whether through disproportionate attacks, failure to distinguish between civilians and combatants, or other violations of IHL.

CONCLUSION

The creation and use of Autonomous Weapon Systems (AWS) present substantial challenges to international humanitarian law and human rights law. As AWS becomes more common on the battlefield, the demand for clarity regarding criminal responsibility increases. This paper argues that individuals or entities that deploy AWS should be held accountable for any harm resulting from these systems. The analysis reveals that existing international legal frameworks are inadequate for addressing the complexities associated with AWS. The inherent lack of human oversight and control in the design of AWS raises significant concerns regarding accountability and responsibility. By imposing liability on those who deploy AWS, we can ensure that both state and non-state actors take necessary precautions to protect civilians and adhere to international law, especially since the development and deployment of AWS violate fundamental principles of distinction and proportionality outlined in international humanitarian law.

This research paper aims to pinpoint the individuals or entities that can be held responsible when AWS are involved in actions leading to violations of international law, such as war crimes or human rights abuses. Given the autonomy of these systems, which can function without direct human intervention, it is essential to determine whether responsibility falls on the developers who program the algorithms, the military commanders who authorize their use, the manufacturers who create these systems, or the states that deploy them. The research intends to examine the extent to which accountability can be assigned to each of these actors and how existing legal and ethical frameworks delineate responsibility.

In light of the identified gaps and ambiguities within current legal frameworks, this paper explored potential reforms or the establishment of new legal mechanisms that can more effectively tackle accountability for violations of international law related to AWS. The objective is to propose concrete legal reforms or new frameworks that can adapt to the rapid advancements in autonomous technology while ensuring compliance with international legal standards.