The Infinite
An International Peer Reviewed / Refereed Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 2 | Issue 6 | June 2025
ISSN: 3048-9539 (Online)
Website: www.theinfinite.in

International Humanitarian Law and Modern Warfare: Challenges in the Age of Autonomous Weapons and Cyber Conflicts

Dr. Ajay Kumar Singh

Associate Professor

Department of Law

K.S. Saket P.G. College, Ayodhya

ARTICLE DETAILS

Research Paper

Keywords :

Autonomous weapons, cyber warfare, international humanitarian law, accountability, Geneva Conventions

ABSTRACT

The transformation of warfare in the 21st century, driven by rapid technological advancements, has introduced profound challenges to the foundational principles of International Humanitarian Law (IHL). Traditional legal norms, developed in the context of conventional warfare, are increasingly being tested by the emergence of novel means and methods of warfare—most notably, autonomous weapons systems (AWS) and cyber operations. These tools, often characterized by speed, precision, and minimal human intervention, have the potential to reshape the conduct of armed conflict in ways previously unimaginable. However, their integration into military strategies also raises pressing legal, ethical, and humanitarian concerns.

This paper critically examines the adequacy of the current international legal framework in addressing the complexities introduced by AWS and cyber warfare. It explores the extent to which the cardinal principles of IHL—namely distinction (between combatants and civilians), proportionality (in the use of force), and military necessity—can be effectively applied in technologically mediated conflicts. The analysis underscores the challenges posed by algorithmic decision-making in AWS, which may lack the contextual judgment necessary to uphold these principles, and the anonymity and attribution difficulties associated with

cyber operations, which complicate compliance and enforcement. Moreover, the paper delves into the increasingly blurred lines of accountability in modern warfare, where both state and non-state actors can deploy sophisticated technologies with potentially devastating consequences. It investigates legal responsibility in scenarios involving machine-driven targeting, decentralized cyber attacks, and hybrid tactics that fall in legal grey zones. Ultimately, the study advocates for comprehensive legal and institutional reforms to reinforce the relevance and robustness of IHL in the digital age. This includes the development of new international treaties or protocols specifically addressing autonomous and cyber weapons, establishing mechanisms for transparent reporting and verification, and mandating meaningful human control over the use of force. Such reforms are essential to safeguard humanitarian principles, ensure accountability, and uphold the rule of law in an increasingly complex and technologically advanced warfare landscape.

1. Introduction

International Humanitarian Law (IHL), also referred to as the Law of Armed Conflict or the Law of War, serves as a vital legal and moral framework aimed at mitigating the human suffering caused by armed conflict. Its central objectives are to protect persons who are not, or are no longer, participating in hostilities—such as civilians, prisoners of war, and the wounded—and to regulate the conduct of hostilities by imposing restrictions on the means and methods of warfare. Core principles such as distinction, proportionality, necessity, and humanity are intended to preserve a balance between military objectives and humanitarian considerations. However, the unprecedented pace of military technological innovation in recent years is posing serious challenges to the traditional application and interpretation of IHL. The emergence of autonomous weapons systems (AWS), capable of selecting and engaging targets without direct human intervention, and cyber warfare tools that can cripple infrastructure or manipulate digital information without firing a single shot, represent a new frontier in the conduct of hostilities. These technologies frequently operate in ways that transcend conventional battlefields and combat scenarios, undermining established legal doctrines rooted in state-centric, physical, and clearly attributable forms of warfare. Autonomous systems, driven by artificial intelligence and machine learning algorithms,

complicate the principle of meaningful human control, raising concerns about accountability for unlawful killings or unintended civilian casualties. In parallel, cyber operations often originate from anonymous or state-sponsored actors, exploiting the digital realm's opacity to conduct attacks with plausible deniability. This challenges the attribution of responsibility—a foundational requirement for enforcing compliance and securing reparations under IHL.

Moreover, these technologies blur the lines between war and peace, combatant and civilian, and state and non-state actors. For example, a cyberattack on a civilian power grid could have military implications without ever involving armed force in the traditional sense, yet its legality under IHL remains contentious. The speed, scale, and unpredictability of these tools further strain mechanisms for real-time decision-making and legal review, making it increasingly difficult to ensure compliance with humanitarian norms in practice.

As such, the growing use of autonomous and cyber capabilities in modern warfare necessitates a re-examination of IHL's existing framework to determine whether it is sufficiently adaptable or in need of reform. Without deliberate and coordinated efforts to clarify, update, or expand the law, there is a risk that the protection of civilians and the accountability of actors in armed conflict will erode in the face of technological advancement.

2. Autonomous Weapons Systems (AWS) and Legal Challenges

Autonomous Weapons Systems refer to machines that can select and engage targets without human intervention. While offering military efficiency, AWS raise several legal and ethical concerns:

2.1 Lack of Human Judgment

IHL requires human judgment in applying the principles of distinction and proportionality. AWS may not be capable of making nuanced decisions, especially in complex combat environments with civilians.

2.2 Attribution of Responsibility

If an AWS commits a violation, it is unclear who is legally accountable – the programmer, the military commander, or the state. This uncertainty risks creating accountability gaps under IHL.

2.3 Compatibility with Existing Treaties

There is no specific treaty banning AWS, though the Martens Clause and Additional Protocol I to the Geneva Conventions emphasize human conscience and international morality, which AWS might contravene.

3. Cyber Warfare and International Humanitarian Law

Cyber operations can disable infrastructure, manipulate data, or conduct espionage, often without direct violence. Their regulation under IHL is contentious due to their covert nature and unpredictable consequences.

3.1 Defining Armed Conflict in Cyberspace

A cyber operation must meet a certain threshold of violence to be classified as an armed conflict. This makes it difficult to trigger the application of IHL, especially when cyber-attacks cause disruption rather than physical destruction.

3.2 Civilian-Military Distinction

Cyber operations often target dual-use systems like communication networks or power grids, blurring the line between civilian and military targets and increasing the risk of civilian harm.

3.3 Attribution Problems

Attributing cyber-attacks to specific state or non-state actors is inherently difficult, complicating enforcement and retaliation under international law.

4. Case Studies

4.1 Israel-Hamas Conflict (2023–2024)

The use of autonomous drones and cyber tools by both sides raises questions on how proportionality and distinction were applied. Investigations by international bodies like the UNHRC emphasized the lack of transparency and accountability.

4.2 Russia-Ukraine War (2022–present)

Cyber-attacks on Ukrainian critical infrastructure were used alongside traditional military operations. These acts showcased how cyber warfare can be used to weaken a state without direct confrontation, raising questions on legal thresholds and responses under IHL.

5. Accountability and the Role of International Institutions

The existing international legal institutions, particularly the International Criminal Court (ICC) and the International Court of Justice (ICJ), play crucial roles in the prosecution and adjudication of serious violations of international law, including war crimes, crimes against humanity, and genocide. However,

when it comes to emerging domains such as autonomous weapons systems (AWS) and cyber warfare, both courts face significant limitations in terms of jurisdiction, attribution, and evidentiary standards.

The ICC, which is mandated to hold individuals criminally accountable, operates on the basis of complementarity and state consent. Many technologically advanced states, particularly those with significant military capabilities, are either not parties to the Rome Statute or have opted out of its jurisdictional provisions, thereby constraining the Court's ability to pursue cases involving the deployment of AWS or state-sponsored cyber operations. Even where jurisdiction exists, the attribution of responsibility in the use of autonomous systems is complex. AWS often involve multiple actors—developers, programmers, commanders, and operators—making it difficult to pinpoint who holds direct criminal liability, especially when harm results from unintended or unpredictable machine behavior.

Similarly, cyber operations are often designed to obscure their origin, employing anonymization techniques, proxies, and false flags. This makes establishing reliable evidence, proving intent, and identifying perpetrators particularly challenging under the evidentiary standards required by international courts. The ICJ, while serving as the principal judicial organ of the United Nations for state-to-state disputes, is likewise hampered by its dependency on state consent and its inability to adjudicate individual criminal responsibility. Its advisory opinions, while authoritative, are not binding in the same manner as ICC verdicts and often lack enforcement mechanisms.

Given these structural and procedural constraints, it has become increasingly clear that current legal mechanisms are ill-equipped to handle the unique challenges posed by AWS and cyber warfare. In light of this, there is growing support among legal scholars and human rights advocates for the creation of new international protocols—possibly under the framework of the Geneva Conventions—to fill this legal void. The existing four Geneva Conventions and their Additional Protocols address various aspects of conventional warfare, but none explicitly regulate autonomous or cyber capabilities.

A potential Fifth Geneva Convention, or a new dedicated protocol, could establish clear norms, responsibilities, and prohibitions concerning the development, deployment, and use of AWS and cyber tools during armed conflict. Such an instrument could mandate meaningful human control, define state obligations for transparency and reporting, create accountability mechanisms, and ensure compliance with IHL principles in the digital and autonomous domain. Furthermore, it could provide a forum for international cooperation, verification procedures, and collective enforcement, thus reinforcing the humanitarian protections that are currently at risk in the face of rapidly evolving warfare technologies.

Ultimately, without such targeted legal innovation, the continued use and expansion of AWS and cyber operations risk creating accountability gaps that could be exploited by state and non-state actors alike—undermining the very foundations of international humanitarian law and the global justice system.

6. Recommendations

6.1. Legal Clarification:

The rapid development of Autonomous Weapon Systems (AWS) and cyber tools has outpaced the existing frameworks of international humanitarian law (IHL) and international legal instruments. The Geneva Conventions, the Hague Regulations, and related protocols were drafted in the context of traditional, kinetic warfare and are ill-equipped to address the unique challenges posed by algorithm-driven systems and intangible cyber operations. Therefore, there is a compelling need to update existing legal instruments or formulate new ones that explicitly govern the development, deployment, and accountability of AWS and cyber capabilities. Legal clarification should include definitions of autonomy in weapon systems, criteria for lawful targeting, accountability structures for violations, and safeguards to protect civilians and critical infrastructure from the unintended consequences of emerging technologies.

6.2. Human Control Mandate:

A foundational principle of international humanitarian law is the preservation of human dignity and the principle of distinction between combatants and civilians. To uphold these principles in the context of automated and algorithmic warfare, it is essential to establish a binding mandate for meaningful human control over all weapons systems. This control must be exercised not only at the point of deployment but also during target selection and engagement. Such a mandate would ensure that humans remain responsible decision-makers in the use of lethal force, prevent moral disengagement, and provide a necessary check against unanticipated actions of autonomous systems. It would also reinforce the concept of command responsibility, thereby strengthening legal and ethical accountability.

6.3. Transparency and State Responsibility:

As the use of AWS and cyber weapons becomes more prevalent, ensuring transparency in state conduct during armed conflict is crucial. States must be compelled to publicly declare the nature and scope of their autonomous and cyber capabilities used in military operations. This transparency serves multiple purposes: it fosters trust among states, deters violations of international law, and enables meaningful international monitoring and verification. Moreover, the principle of state responsibility must be unequivocally applied—states should bear full legal and moral responsibility for the consequences of their

deployment of AWS and cyber tools, whether these are carried out directly or via proxies. Establishing such a responsibility framework would reinforce deterrence and provide victims with avenues for redress.

6.4. International Treaty on Cyber Warfare:

Despite the growing frequency and severity of cyber operations during armed conflict, there is currently no comprehensive international treaty that governs cyber warfare. This legal vacuum leaves room for ambiguity and exploitation. A multilateral treaty under the auspices of the United Nations should be urgently negotiated to define the limits and permissible uses of cyber capabilities in the context of armed conflict. The treaty should address issues such as the protection of civilian infrastructure (e.g., hospitals, power grids), the prohibition of cyber attacks on humanitarian operations, norms for attribution, and the application of proportionality and necessity in cyber operations. It should also include mechanisms for enforcement, dispute resolution, and the imposition of sanctions for non-compliance. Such a treaty would provide much-needed clarity and cohesion in the international legal regime governing modern conflict.

7. Conclusion

Modern warfare is evolving at an unprecedented pace, driven by rapid technological advancements such as autonomous weapon systems (AWS), artificial intelligence, and sophisticated cyber capabilities. These innovations are transforming the nature of armed conflict—from physical battlegrounds to virtual arenas—where decisions may be made in milliseconds by algorithms rather than human commanders. However, the legal frameworks that govern armed conflict, particularly International Humanitarian Law (IHL), have not kept pace with these changes. The existing norms were primarily designed to regulate conventional warfare and are increasingly strained under the weight of modern, tech-driven threats.

To preserve the humanitarian ethos that lies at the heart of IHL—protecting civilians, ensuring proportionality, and maintaining accountability—it is imperative that international legal norms evolve proactively. Legal inertia in the face of emerging technologies risks undermining decades of progress in humanizing warfare and upholding the principles of distinction, necessity, and humanity. Without clear legal guidance, there is a heightened risk of unlawful targeting, diminished accountability, and increased civilian suffering.

The international community must therefore act collectively and decisively to ensure that technological advancements do not outpace the ethical and legal obligations that govern the conduct of hostilities. This includes updating existing treaties, drafting new international agreements specifically addressing autonomous and cyber warfare, and reinforcing the mandate for human oversight in the use of force. Only

through anticipatory and inclusive legal development can we ensure that innovation in warfare does not come at the expense of human dignity and fundamental rights.

References

1. Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War, 12 August 1949.
2. Protocol Additional to the Geneva Conventions of 12 August 1949 (Protocol I), 8 June 1977.
3. United Nations Charter, 26 June 1945.
4. Martens Clause, Preamble to the 1899 Hague Convention II with Respect to the Laws and Customs of War on Land.
5. International Committee of the Red Cross. (2016). *Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons*.
6. United Nations. (2021). *Report of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems*.
7. Schmitt, M. N. (2017). Autonomous weapons and international humanitarian law: A reply to the critics. *Harvard National Security Journal*, 8, 1–32.
8. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. (2017). NATO Cooperative Cyber Defence Centre of Excellence.
9. Sassòli, M. (2019). *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare*. Edward Elgar Publishing.
10. Asaro, P. (2012). On banning autonomous weapon systems: Human rights, automation, and the dehumanization of lethal decision-making. *International Review of the Red Cross*, 94(886), 687–709.
11. Boothby, W. (2009). *Weapons and the Law of Armed Conflict*. Oxford University Press.
12. Daskal, J. (2015). The un-territoriality of data. *Yale Law Journal*, 125(2), 326–398.
13. Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford University Press.
14. Heyns, C. (2013). Autonomous weapons and the right to life: An international law perspective. Report to the UN Human Rights Council.

15. Melzer, N. (2013). Human rights implications of the usage of drones and unmanned robots in warfare. European Parliament Directorate-General for External Policies.
16. International Law Commission. (2001). *Draft Articles on Responsibility of States for Internationally Wrongful Acts*.
17. Human Rights Watch. (2012). *Losing Humanity: The Case Against Killer Robots*.
18. United Nations Institute for Disarmament Research. (2014). *The Weaponization of Increasingly Autonomous Technologies*.
19. Chatham House. (2020). *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*.
20. International Committee of the Red Cross. (2018). *Ethical and Legal Concerns Surrounding Autonomous Weapons*.