YourLawArticle

Open Access Law Journal, ISSN (O): 3049-0057

Editor-in-Chief – Prof. (Dr.) Amit Kashyap; Publisher – Reet Parihar

Asymmetric Warfare as a Fifth-Generation Human Rights Challenge

Advocate Sanchari Biswas, 1st Year of LL.M in Human Rights, Department Of Law University of Calcutta.

Published on: 14th July 2025

Abstract

Fifth-generation warfare (5GW) has emerged as the dominant form of conflict in the 21st century, radically transforming the nature of warfare and its legal and humanitarian consequences. Unlike conventional armed conflicts, which involve identifiable state actors, formal declarations of war, and kinetic force, 5GW is characterized by the use of cyberattacks, disinformation, psychological operations, artificial intelligence (AI), and autonomous weapon systems. These non-kinetic tools allow both state and non-state actors to operate below the threshold of traditional armed conflict, often with plausible deniability and minimal physical presence. The anonymity and decentralization inherent in 5GW make it difficult to identify perpetrators, assign state responsibility, or classify combatants according to existing legal frameworks. As a result, the foundational principles of international humanitarian law (IHL), the Geneva Conventions, and international criminal law built for conflicts between nations , struggle to regulate these emerging threats. Civilians are increasingly targeted or used as instruments of war, blurring the line between combatant and non-combatant. This paper explores how fifth-generation warfare challenges traditional concepts of victimhood, erodes the mechanisms of accountability, complicates questions of legal jurisdiction, and exposes the limitations of current legal protections. It argues for a reimagined human rights framework that addresses the unique threats posed by modern, hybrid, and information-centric conflicts.

Key Words: *Fifth-generation warfare, cyberattacks, legal framework, information warfare, jurisdiction, civilian targeting*

INTRODUCTION

Fifth-generation warfare (5GW) is no longer a theoretical construct discussed solely in military academies or think tanks, it has become an operational reality influencing global conflict dynamics. Unlike conventional kinetic warfare, 5GW employs non-physical, strategic mechanisms such as information manipulation, cyberattacks, psychological operations, and decentralized militant actions, often orchestrated without formal declarations of war or identifiable combatants.[1] These tools allow both state and non-state actors to pursue political or military objectives through invisible, often deniable means that challenge the very foundation of traditional warfare theory.[2]

Information warfare, for instance, targets public perception and civic trust through disinformation, deepfake technology, and algorithmic manipulation of social media feeds.[3] Similarly, cyberattacks can paralyze critical infrastructure like hospitals, energy grids, financial systems—without a single shot fired. Psychological operations weaponize fear, confusion, and emotional destabilization, often using online platforms to induce mass panic or erode democratic cohesion.[4] Decentralized militant actions, carried out by loosely affiliated cells or individuals radicalized online, further complicate attribution and legal accountability.

These asymmetrical confrontations bypass traditional, state-centred warfare mechanisms codified in international humanitarian law (IHL) and the Geneva Conventions, which were primarily designed for state-versus-state conflicts involving identifiable armed forces. The rules of engagement, protections for civilians, and norms of accountability built into existing legal frameworks struggle to accommodate actors who operate in digital shadows, who may not wear uniforms, and who defy geographic borders.[5]

As a result, civilians, civilian infrastructure, and democratic institutions are now not just collateral damage but often the primary targets or battlegrounds of 5GW. This shift has profound implications for international human rights law and humanitarian norms. It necessitates a thorough re-evaluation of accountability mechanisms, jurisdictional scope, and the classification and protection of victims in modern conflict scenarios.[6] Without such reform, both state and non-state actors can exploit legal grey zones, eroding the universality and enforceability of human rights protections in contemporary

[1] Daniel Abbott, *The Handbook of Fifth-Generation Warfare* (Nimble Books 2010) 12–14.
[2] Andreas Krieg and Jean-Marc Rickli, *Surrogate Warfare: The Transformation of War in the Twenty-First Century* (Georgetown University Press 2019) 5–7.
[3] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (Farrar, Straus and Giroux 2020) 9–12.
[4] United Nations Institute for Disarmament Research (UNIDIR), *The Cyber Index: International Security Trends and Realities* (2013) 31–33.
[5] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press 2017) 3–4.
[6] Michael Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) 38–42.

armed conflict.

Understanding Fifth-Generation Warfare

Fifth-generation warfare (5GW) represents a paradigm shift from conventional military engagements. It is defined not by superior firepower or troop movements, but by disruption, ambiguity, and psychological dominance. At its core, 5GW is characterized by:

- **Asymmetry**: Power disparities are central to 5GW. Small, resource-poor groups can leverage cyber capabilities or information campaigns to challenge state actors. For example, insurgent groups may exploit soft targets or conduct cyber intrusions into national defense systems, thus achieving disproportionate impact with minimal conventional force.[7]
- **Decentralization**: Traditional warfare depends on structured command chains. In contrast, 5GW often involves non-hierarchical, dispersed networks such as terrorist cells, online radical groups, and hacker collectives , making them harder to detect, disrupt or negotiate with.These actors often self-radicalize or operate semi-autonomously, without formal state affiliations or clear political objectives.
- **Psyops and Narrative Warfare**: Fifth-generation conflict often centers around manipulating perceptions rather than destroying assets. Narrative warfare sometimes termed "cognitive warfare" involves spreading disinformation, conspiracy theories, and fake news to erode public trust in institutions, sow division, and destabilize societies from within.[8] Tools such as deepfakes, troll farms, and algorithmically targeted messaging serve to amplify confusion and dissent.
- **Cyber and AI Tools**: Cyberattacks have become routine instruments of political and economic coercion. State and non-state actors exploit vulnerabilities in infrastructure, finance, healthcare, and even electoral systems to paralyze civilian life or gain strategic advantage.[9] Artificial intelligence adds further complexity, automating decision-making, surveillance, and even lethal targeting in autonomous weapons systems.[10]
- **Civilian Targeting**: In 5GW, civilians are no longer peripheral. They are both targets and tools subject to psychological operations, surveillance, and coercive messaging. Critical

[7] Daniel Abbott, *The Handbook of Fifth-Generation Warfare* (Nimble Books 2010) 18.
[8] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (Farrar, Straus and Giroux 2020) 73–75.
[9] United Nations Institute for Disarmament Research (UNIDIR), *The Cyber Index: International Security Trends and Realities* (2013) 28–31.
[10] Rafia Islam and Azmine Wasi, 'Balancing Power and Ethics: A Framework for Addressing Human Rights Concerns in Military AI' (2024) https://arxiv.org/abs/2404.10047 accessed 14 July 2025.

civilian infrastructure like hospitals, communication networks, and power grids become strategic targets, with the boundary between combatant and non-combatant often ignored.[11]

These methods collectively blur the lines between peace and war, combatant and civilian, lawful and unlawful. The nature of 5GW makes it harder to invoke traditional legal safeguards because attacks often lack clear attribution, occur outside of conventional warzones, and take place during ostensible "peacetime."[12]

The Evolution of Human Rights in Armed Conflict

Human rights protections in times of war have historically been guided by a corpus of international law built around **state-centric armed conflict**. The foundational instruments include:

- **The Geneva Conventions**: Enacted in 1949, these treaties establish standards for humane treatment of civilians and combatants in international and non-international armed conflict.
- **International Humanitarian Law (IHL)**: IHL sets out the principles of distinction, proportionality, and necessity, obligating warring parties to avoid civilian harm and unnecessary suffering.
- **International Criminal Law (ICL)**: Through institutions like the International Criminal Court (ICC), ICL holds individuals criminally liable for war crimes, genocide, and crimes against humanity.
- **Customary International Law**: Over time, certain norms such as the prohibition of torture and targeting civilians have acquired binding legal force even without formal treaty codification.

However, these regimes were conceived during an era when warfare was typically **state-on-state**, with clear lines of battle and defined belligerents. Fifth-generation warfare radically complicates this structure in three critical areas:

- **State Responsibility**: Attribution is foundational to accountability. But how can international law assign responsibility when a cyberattack on a civilian hospital originates from an anonymous group with no declared affiliation? Existing doctrines of state responsibility struggle to apply to non-state actors acting independently or with covert **support**.The International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts presuppose a clear link between action and state control rare

[11] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press 2017) 54–55.
[12] Michael Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) 4.

in 5GW.[13]

- **Combatant Status**: The legal distinction between combatants and civilians determines who can be lawfully targeted and who qualifies for prisoner-of-war status. In 5GW, actors often operate without uniforms, military hierarchy, or even clear objectives. Are hackers who disrupt energy grids lawful combatants? Should cyber warriors receive POW status if captured? These questions remain unresolved, straining the interpretative capacity of IHL.[14]
- **Jurisdiction**: Cyber operations routinely transcend national boundaries. An attack launched in one state may be routed through several others and impact victims globally. Traditional jurisdictional rules based on territoriality or nationality are insufficient to deal with **cross-border, virtual warfare**. This creates enforcement gaps and raises concerns about **forum shopping**, digital impunity, and extraterritorial overreach.[15]

In sum, fifth-generation warfare undermines the traditional pillars of international law. The emphasis on anonymity, psychological influence, and technological disruption calls for a **recalibration of legal doctrines** to ensure that fundamental human rights are not eroded under the cover of digital ambiguity.

Asymmetric Warfare and Human Rights Violations

Fifth-generation warfare (5GW) introduces a radically different threat matrix, one that targets civilians as both instruments and victims of conflict. The unconventional nature of 5GW has led to novel human rights violations that existing frameworks struggle to address effectively. These violations often occur outside conventional combat zones, during times not formally recognised as war, and through tools such as code, content, or AI that were never contemplated in the drafting of foundational treaties.

- **Cyberattacks on Hospitals and Civilian Infrastructure**

Cyber operations that disable healthcare systems, water supplies, or power grids constitute clear violations of the right to health, security, and privacy under international human rights law. For example, ransomware attacks on hospitals during the COVID-19 pandemic had life-threatening implications and disrupted essential health services.The International Committee of the Red Cross (ICRC) has affirmed that such attacks may constitute violations of both international humanitarian law and the right to life.When hospitals are rendered inoperative not by bombs but by keystrokes,

[13] Oona Hathaway and others, 'The Law of Cyber-Attack' (2012) 100 *California Law Review* 817, 842–844.
[14] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, with commentaries (2001) UN Doc A/56/10, arts 2–8.
[15] Gary D Solis, *The Law of Armed Conflict: International Humanitarian Law in War* (2nd edn, CUP 2016) 199–201.

the distinction between physical and non-physical aggression becomes legally and morally untenable.[16]

- **Disinformation Campaigns**

Narrative warfare and disinformation campaigns disrupt democratic participation, erode the right to freedom of expression, and infringe upon the public's right to truthful information. Coordinated inauthentic behaviour such as deepfake videos, bot-driven misinformation, or targeted propaganda can skew elections, inflame ethnic tensions, and discredit public institutions. These tactics may constitute psychological manipulation on a mass scale, and when state-sponsored, could amount to **information warfare** in breach of democratic guarantees under international covenants like the ICCPR.[17]

- **Drone Strikes and Autonomous Weapons**

The increasing reliance on unmanned aerial vehicles (UAVs) and semi-autonomous weapons systems introduces dangerous gaps in accountability. When a drone strike kills civilians, it often remains unclear who authorised the strike, whether the targeting algorithms were properly calibrated, or whether adequate precautions were taken to avoid collateral damage.Such deaths directly challenge **Article 6 of the ICCPR**, which protects the right to life and places high thresholds on state use of lethal force.The use of fully autonomous weapons lacking meaningful human oversight risks violating the principles of necessity and proportionality under IHL.[18]

- **Psychological Warfare**

Perhaps the most insidious aspect of 5GW is its cognitive reach. Psychological operations designed to destabilise mental resilience can induce trauma, fear, and confusion among populations.Tactics include inducing mass panic via false alarms, weaponised rumors, or targeted psychological harassment through digital means. Although not yet clearly addressed in legal terms, such operations arguably infringe on the **right to mental health**, recognised in instruments such as the **ICESCR** and emerging normative frameworks.These tactics weaponise the mind, not the body, creating invisible wounds that law has yet to adequately redress.[19]

Legal and Ethical Dilemmas

[16] UNGA, 'Report of the Special Rapporteur on the Right to Health' (A/HRC/44/48, 2020).
[17] ICRC, 'International Humanitarian Law and Cyber Operations During Armed Conflicts' (2021) https://www.icrc.org accessed 14 July 2025.
[18] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (FSG 2020) 9.
[19] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) arts 19, 25.

The advent of 5GW has exposed **structural weaknesses in international law** and raised a host of ethical questions that existing institutions are ill-equipped to resolve.[20]

- **Attribution Gap**

One of the central challenges of 5GW is attribution. Cyberattacks and information warfare are frequently conducted via anonymised networks, proxy servers, or non-state entities acting with plausible deniability.Without credible attribution, it becomes nearly impossible to hold actors accountable or to apply the laws of armed conflict and human rights jurisprudence effectively.

- L**egal Vacuum**

The law of armed conflict is primarily structured around clearly identifiable roles combatants, civilians, commanders. However, many 5GW actors occupy a **grey zone**, being neither formal soldiers nor innocent civilians. Hackers, autonomous algorithms, and disinformation agents often fall outside legal definitions, creating **accountability vacuums**.As a result, individuals who inflict significant harm may evade any legal responsibility, and victims are left without redress.

- **Humanitarian Access**

Hybrid conflict zones often restrict access to humanitarian actors. In 5GW, warfare can unfold in encrypted digital platforms or urban environments where neutral monitoring becomes impossible.Cyberattacks may prevent international organisations from tracking violations or delivering assistance, thereby compromising victims' access to justice and care.

- **Over-Securitisation**

In response to these threats, some states have adopted extreme countermeasures: widespread surveillance, censorship, suppression of dissent, or emergency powers under counterterrorism pretexts.While aimed at combating non-state threats, these actions often result in significant human rights violations against their own populations. The challenge lies in balancing security imperatives with civil liberties in an increasingly paranoid digital age.

Toward a Fifth-Generation Human Rights Framework

A new paradigm of rights protection is needed one that responds to the **technological, psychological, and informational dimensions** of modern warfare. Several key reforms are

[20] UNHRC, 'Report on the Promotion and Protection of Human Rights while Countering Terrorism' (A/HRC/40/52, 2019).

essential[21]:

Update Legal Instruments : There is an urgent need to supplement or revise the Geneva Conventions to include binding protocols on cyberwarfare, AI-guided weaponry, and psychological operations. These updates must reflect the challenges posed by non-kinetic warfare, particularly the use of digital and cognitive tools.

International Attribution Mechanisms: The creation of international cyber forensic bodies is vital. Such institutions could be modelled after existing UN panels of experts and operate with a mandate to attribute cyber and narrative attacks, providing legally usable evidence for national or international courts.

Civilian Protections in Psychological Warfare: International law must now recognise the psychological dimension of war. Protections for cognitive sovereignty and emotional integrity should be codified, including the right not to be subjected to weaponised misinformation or psychological harm.

Ethical AI Governance: Autonomous weapon systems must be subject to meaningful human oversight. Legal frameworks should ensure that decisions about life and death are not delegated to algorithms, aligning the development of military AI with international human rights standards.

Digital Rights Expansion : Digital rights including data privacy, internet access, and information integrity should be recognised as human rights. Legal instruments must prohibit state and non-state actors from interfering with the public's right to accurate information and safe digital spaces.

7. Implementing a Fifth-Generation Human Rights Regime

Responding to the evolving nature of warfare requires **institutional and cultural transformation**[22]:

- **Legal Reform and Expansion**: Member states should convene under the UN to codify digital and psychological rights, integrating these into the human rights architecture of bodies such as the Human Rights Council or OHCHR.
- **Cyber Accountability Mechanisms**: Establishment of Cyber Accountability Tribunals or chambers within existing courts like the ICC would provide jurisdiction for major cyber and cognitive attacks.

[21] UNHRC, 'Report on the Promotion and Protection of Human Rights while Countering Terrorism' (A/HRC/40/52, 2019).
[22] UNGA Res 73/27 (2018) on the Promotion of a Culture of Tolerance and Peace in the Digital Age.

- **Recognition of Digital and Psychological Rights**: Treaties should formalise rights related to **mental well-being, truthful communication, and data dignity**.
- **Global Governance of Autonomous Weapons**: Through frameworks like the Convention on Certain Conventional Weapons (CCW), multilateral treaties should seek to regulate or prohibit autonomous systems that act outside human control.
- **Strengthened Civil Society and Media Literacy**: Investing in education programs, journalism training, and public resilience against misinformation can inoculate societies from the most harmful effects of narrative warfare.

8. Conclusion

Fifth-generation warfare marks a critical inflection point in the evolution of armed conflict. No longer confined to borders, troops, or traditional weapons, today's wars are fought through information, algorithms, and emotional influence. Civilians are not merely caught in the crossfire. They are increasingly the target and terrain of battle.

The tools of 5GW like cyberattacks, drones, psychological operations have outpaced legal frameworks constructed in an analogue age. Without substantive reform, international law risks obsolescence. The time has come to construct a robust, adaptable, and ethically sound human rights regime, one that integrates digital rights, technological safeguards, and accountability mechanisms suited for the realities of the 21st century. Only then can we ensure that human dignity endures in the shadow of invisible wars.

Reference

Abbott D, The Handbook of Fifth-Generation Warfare (Nimble Books 2010)

Hathaway O and others, 'The Law of Cyber-Attack' (2012) 100 California Law Review 817

International Committee of the Red Cross (ICRC), 'International Humanitarian Law and Cyber Operations During Armed Conflicts' (2021) https://www.icrc.org accessed 14 July 2025

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171

International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries (2001) UN Doc A/56/10

Islam R and Wasi A, 'Balancing Power and Ethics: A Framework for Addressing Human Rights Concerns in Military AI' (2024) https://arxiv.org/abs/2404.10047 accessed 14 July 2025

Krieg A and Rickli JM, Surrogate Warfare: The Transformation of War in the Twenty-First Century (Georgetown University Press 2019)

Rid T, Active Measures: The Secret History of Disinformation and Political Warfare (Farrar, Straus and Giroux 2020)

Schmitt M (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press 2017)

Solis GD, The Law of Armed Conflict: International Humanitarian Law in War (2nd edn, Cambridge University Press 2016)

United Nations General Assembly (UNGA), 'Report of the Special Rapporteur on the Right to Health' (A/HRC/44/48, 2020)

UNGA Res 73/27 (2018) on the Promotion of a Culture of Tolerance and Peace in the Digital Age

United Nations Human Rights Council (UNHRC), 'Report on the Promotion and Protection of Human Rights while Countering Terrorism' (A/HRC/40/52, 2019)

United Nations Institute for Disarmament Research (UNIDIR), The Cyber Index: International Security Trends and Realities (2013)