

Changing Nature of Armed Conflict: International Humanitarian Law in the Age of Hybrid Warfare

Dr. Shalini Saxena¹, Prof. (Dr.) Ashish Verma², Dr. Shubham Singh Bagla³, Dr. Jitendra Kumar Gautam⁴

¹HOD & Associate Professor, Faculty of Law, SRM University, Sonapat, Haryana

²Professor and Dean, Chitkara School of Law, Chitkara University, Chandigarh

³Assistant Professor, Faculty of Law, SRM University, Sonapat Haryana

⁴Assistant Professor, Faculty of Law, SRM University, Sonapat, Haryana

Abstract

The transformation of warfare in the twenty-first century has challenged the traditional understanding of armed conflict and the legal frameworks governing it. Contemporary conflicts increasingly exhibit characteristics of hybrid warfare, a multidimensional strategy that combines conventional military operations with irregular tactics, cyber warfare, information manipulation, economic coercion, and the involvement of proxy actors. Such conflicts often blur the distinction between war and peace, state and non-state actors, and military and civilian targets. Consequently, these developments have generated significant legal and humanitarian concerns regarding the adequacy and applicability of International Humanitarian Law (IHL), which was primarily developed to regulate conventional interstate wars.

This article examines the changing nature of armed conflict and critically evaluates the capacity of IHL to address the complexities posed by hybrid warfare. It analyses the legal foundations of IHL, including the Geneva Conventions of 1949 and their Additional Protocols, and explores whether existing principles such as distinction, proportionality, military necessity, and humanity remain effective in contemporary conflict environments. Particular attention is paid to cyber operations, disinformation campaigns, the role of non-state actors and proxy forces, and the emergence of grey-zone warfare. Through an examination of recent conflicts, including the Russia–Ukraine war and the Israel–Hamas conflict, the article assesses the practical difficulties associated with classification, attribution, accountability, and enforcement.

The study argues that although International Humanitarian Law possesses sufficient normative flexibility to regulate many aspects of hybrid warfare, the absence of clear legal standards concerning cyber operations, information warfare, and indirect participation in hostilities necessitates interpretative developments and stronger mechanisms of international cooperation. Strengthening compliance and adapting legal norms to technological realities are essential to preserving humanitarian values in modern warfare.

Keywords: Hybrid Warfare, International Humanitarian Law, Cyber Warfare, Non-State Actors, Armed Conflict.

INTRODUCTION

The nature of armed conflict has undergone profound transformation in the twenty-first century. While conventional wars between sovereign states dominated much of the nineteenth and twentieth centuries, contemporary conflicts increasingly involve complex interactions among state actors, non-state groups, cyber capabilities, proxy forces, and information warfare. These developments have challenged traditional notions of warfare and raised significant questions regarding the continued effectiveness and applicability of International Humanitarian Law (IHL), the body of law intended to regulate armed conflicts and minimize human suffering.

International Humanitarian Law, often referred to as the law of armed conflict, is founded primarily upon the four Geneva Conventions of 1949 and their Additional Protocols. Its central objective is to protect persons who are not, or are no longer, participating in hostilities and to regulate the means and methods of warfare. The fundamental principles of humanity, distinction, proportionality, military necessity, and precaution have served as the cornerstone of humanitarian regulation for decades. However, these principles were developed largely in the context of conventional interstate warfare and therefore face unprecedented challenges when confronted with the realities of hybrid conflict.¹

Hybrid warfare has emerged as one of the most significant strategic phenomena in modern international relations. Although there is no universally accepted definition, hybrid warfare generally refers to the coordinated use of conventional military force alongside irregular tactics, cyber-attacks, disinformation campaigns, economic pressure, proxy groups, and political subversion to achieve strategic objectives. Such methods allow states and non-state actors to operate below the threshold of traditional warfare, thereby creating ambiguity regarding the existence of armed conflict and complicating the application of international legal norms. The International Committee of the Red Cross (ICRC) has noted that "hybrid threats" and "hybrid warfare" encompass a broad spectrum of military and non-military activities, including covert and overt operations, cyber measures, and information campaigns, which must be assessed under existing legal criteria governing armed conflict.²

The increasing complexity of armed conflict has been accompanied by the proliferation of non-state actors. Armed groups, private military companies, transnational terrorist organizations, and proxy militias have become central participants in many contemporary conflicts. Unlike traditional state actors, these entities frequently operate across national borders and often lack clearly identifiable command structures, making attribution and accountability difficult. Conflicts in Syria, Libya, Yemen, and Ukraine illustrate how state and non-state actors interact in highly fragmented environments where legal responsibilities are often obscured. The rise of such actors has prompted scholars and practitioners to reconsider the distinction between international armed conflicts and non-international armed conflicts and to question whether existing classifications adequately reflect present realities.

Another significant dimension of contemporary warfare is cyberspace. Cyber operations have become increasingly integrated into military strategies and possess the capacity to disrupt critical infrastructure, communication systems, healthcare networks, and financial institutions. Unlike conventional kinetic attacks, cyber operations may produce devastating consequences without physical destruction or immediate loss of life. Their transnational nature, difficulties of attribution, and uncertain legal status present substantial challenges for international law. Although many scholars argue that existing IHL principles apply to cyber operations conducted during armed conflicts, there remains considerable debate concerning the threshold at which cyber activities constitute an armed attack and trigger the applicability of humanitarian norms. The ICRC has repeatedly emphasized that digital technologies and cyber operations create new humanitarian risks while remaining subject to existing legal principles.

The Russia–Ukraine conflict has demonstrated the growing relevance of hybrid warfare in contemporary strategic practice. Military operations have been accompanied by extensive cyber-attacks, disinformation campaigns, economic sanctions, proxy activities, and the use of emerging technologies such as drones and satellite communications. Similarly, the Israel– Hamas conflict has highlighted the challenges associated with urban warfare, information operations, and the protection of civilians in densely populated areas. These examples illustrate that modern conflicts are characterized not merely by kinetic engagements but by multidimensional

¹ International Humanitarian Law and the Challenges of Contemporary Armed Conflicts | International Committee of the Red Cross, (Nov. 13, 2015), <https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts>.

² 2019 ICRC Report on IHL and the Challenges of Contemporary Armed Conflicts | International Committee of the Red Cross, (Nov. 22, 2019), <https://www.icrc.org/en/document/icrc-report-ihl-and-challenges-contemporary-armed-conflicts>.

interactions involving political, economic, informational, and technological instruments. Such developments have blurred the traditional distinction between civilian and military domains, thereby complicating the application of humanitarian protections and increasing risks to civilian populations.

The changing nature of warfare has also generated concerns regarding the adequacy of existing enforcement mechanisms. Although the Geneva Conventions enjoy universal ratification, compliance with IHL remains inconsistent. The absence of effective international enforcement institutions and the political limitations of international criminal accountability have often resulted in impunity for violations. Moreover, hybrid warfare strategies deliberately exploit legal grey areas and seek to avoid clear attribution, thereby undermining traditional mechanisms of responsibility and accountability. Consequently, scholars have increasingly debated whether new treaties are necessary or whether existing norms possess sufficient flexibility to adapt to contemporary challenges.

The International Committee of the Red Cross has consistently maintained that International Humanitarian Law remains capable of addressing many modern challenges, provided that its principles are interpreted and implemented in good faith. According to the 2024 ICRC Report on International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, concepts such as hybrid warfare and proxy warfare do not require entirely new legal frameworks; rather, existing rules should be applied objectively based on the facts of each situation.³ Nevertheless, emerging technologies and unconventional methods of warfare necessitate further clarification and development to preserve the humanitarian objectives underlying IHL.⁴ Against this background, the present study seeks to examine the changing character of armed conflict and assess the effectiveness of International Humanitarian Law in the age of hybrid warfare. It analyses the conceptual foundations of hybrid warfare, explores the applicability of IHL to contemporary conflicts, and evaluates challenges associated with cyber operations, information warfare, non-state actors, and accountability. Through an examination of recent conflicts and emerging technologies, the article aims to determine whether existing humanitarian law is sufficiently adaptable to contemporary realities or whether further normative developments are required to ensure the continued protection of human dignity in armed conflict.⁵

CONCEPTUAL FRAMEWORK OF HYBRID WARFARE

The concept of hybrid warfare has emerged as one of the most debated themes in contemporary security studies and international law. Although the term gained prominence during the early twenty-first century, the strategic blending of conventional and unconventional methods is not entirely new. Historical examples ranging from the Napoleonic Wars to insurgencies during the Cold War demonstrate that states and non-state actors have often employed combinations of military force, propaganda, irregular warfare, and political influence. What distinguishes modern hybrid warfare is the unprecedented integration of these instruments with cyber capabilities, information technologies, economic coercion, and proxy actors.

The term "hybrid warfare" was popularized by Frank G. Hoffman, who defined it as the simultaneous and adaptive use of conventional weapons, irregular tactics, terrorism, and criminal activities by state and non-state actors to achieve political objectives. According to Hoffman, future conflicts would increasingly involve adversaries

³ International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (2024)

<https://www.icrc.org/en/publication/international-humanitarian-law-and-challenges-contemporary-armed-conflicts-building>

⁴ International Committee of the Red Cross, *Contemporary Challenges for IHL* (2013) <https://www.icrc.org/en/document/contemporary-challenges-ihl>

⁵ International Review of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (2025) <https://international-review.icrc.org/articles/reports-and-documents-ihl-and-the-challenges-of-contemporary-armed-conflicts-927>

employing diverse modes of warfare within the same battlespace, thereby blurring distinctions between regular and irregular warfare.⁶

Unlike traditional warfare, hybrid warfare is characterized by ambiguity. It often operates below the threshold of formally declared armed conflict and seeks to exploit legal, political, and psychological vulnerabilities. The North Atlantic Treaty Organization (NATO) describes hybrid threats as a combination of military and non-military means including cyber-attacks, disinformation, economic pressure, espionage, and the use of proxy forces intended to destabilize societies and undermine state institutions.⁷

Hybrid warfare generally includes the following components:

(a) Conventional Military Operations

These involve the use of regular armed forces equipped with modern weaponry and organized command structures.

(b) Irregular Warfare

Insurgencies, guerrilla tactics, and covert operations conducted by proxy groups constitute significant elements of hybrid strategies.

(c) Cyber Operations

Cyber-attacks targeting critical infrastructure, communication systems, and financial institutions have become essential instruments of contemporary warfare.

(d) Information Warfare

Manipulation of public opinion through propaganda, fake news, social media campaigns, and psychological operations seeks to influence political outcomes and weaken adversaries.

(e) Economic Coercion

Sanctions, energy dependency, trade restrictions, and economic pressure are frequently used to supplement military objectives.

The Russia-Ukraine conflict illustrates how these dimensions are integrated simultaneously. Military operations have been accompanied by cyber-attacks, information campaigns, economic sanctions, and proxy activities, demonstrating the multidimensional character of modern warfare.⁸ Consequently, hybrid warfare challenges traditional distinctions between war and peace, civilian and military targets, and state and non-state actors, thereby raising significant legal questions regarding the applicability of International Humanitarian Law.

Evolution of Armed Conflict

Throughout history, armed conflicts have undergone significant transformations in response to technological, political, and social developments.

1. Classical Warfare

Classical warfare primarily involved organized military engagements between sovereign states. The Peace of Westphalia (1648) established the modern state system, within which interstate wars became the dominant form

⁶ Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Potomac Institute for Policy Studies, 2007) https://potomac institute.org/images/stories/publications/potomac_hybridwar_0108.pdf

⁷ NATO, *Countering Hybrid Threats* https://www.nato.int/cps/en/natohq/topics_156338.htm

⁸ International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (2024) <https://www.icrc.org/en/publication/international-humanitarian-law-and-challenges-contemporary-armed-conflicts-building>

of conflict. During this period, military confrontations generally occurred between identifiable armed forces operating under established command structures.

2. Industrial Warfare

The nineteenth and twentieth centuries witnessed industrialized warfare characterized by mass mobilization and technological innovations. The First and Second World Wars demonstrated the devastating effects of mechanized warfare, aerial bombardment, and total war. These experiences prompted the development of the Geneva Conventions of 1949 and subsequent humanitarian norms.⁹

3. Cold War and Proxy Conflicts

During the Cold War, superpower rivalry often manifested through proxy wars in Korea, Vietnam, Afghanistan, and Africa. These conflicts blurred the distinction between international and non-international armed conflicts and involved ideological struggles alongside military engagements.

4. Rise of Non-State Actors

The post-Cold War era witnessed increasing participation by terrorist organizations, insurgent groups, and transnational armed movements. The September 11 attacks and subsequent "Global War on Terror" transformed the international security environment and brought non-state actors to the forefront of contemporary conflicts.¹⁰

5. Fourth Generation Warfare

William Lind's theory of Fourth Generation Warfare emphasizes decentralized networks, asymmetric tactics, and psychological operations. The distinction between civilians and combatants becomes increasingly blurred, and the battlefield extends into cyberspace, media, and economic domains.¹¹

6. Emergence of Hybrid Warfare

The twenty-first century has witnessed the convergence of conventional military operations with cyber warfare, artificial intelligence, information operations, and proxy warfare. The Russia-Ukraine war, Syrian Civil War, and conflicts in the Middle East demonstrate the growing significance of hybrid threats. The changing nature of warfare necessitates a reassessment of legal frameworks originally designed for conventional interstate wars.

APPLICABILITY OF INTERNATIONAL HUMANITARIAN LAW TO HYBRID WARFARE

International Humanitarian Law regulates armed conflicts through treaties and customary international law. Its principal sources include:

- The Four Geneva Conventions of 1949.
- Additional Protocol I (1977).
- Additional Protocol II (1977).
- Customary International Humanitarian Law.
- Hague Regulations of 1907.

One of the most important questions raised by hybrid warfare concerns whether existing IHL remains applicable to modern conflicts. The International Committee of the Red Cross has consistently maintained that IHL applies

⁹ Geneva Conventions of 1949 <https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949>

¹⁰ United Nations Security Council Resolution 1373 (2001) <https://digitallibrary.un.org/record/449023>

¹¹ William S. Lind et al., "The Changing Face of War: Into the Fourth Generation", *Marine Corps Gazette* (1989) <https://www.mca-marines.org/wp-content/uploads/The-Changing-Face-of-War-Into-the-Fourth-Generation.pdf>

whenever the factual criteria for armed conflict are fulfilled, irrespective of labels such as "hybrid warfare" or "grey-zone conflict."¹²

Classification of Armed Conflict

International Humanitarian Law distinguishes between:

(a) International Armed Conflicts (IAC)

Article 2 common to the Geneva Conventions provides that an international armed conflict exists whenever there is armed force between two or more states.

(b) Non-International Armed Conflicts (NIAC)

Common Article 3 applies to conflicts involving organized armed groups and governmental forces within a state. Hybrid warfare often combines both categories. State-sponsored militias, private military companies, and proxy groups complicate the determination of legal status and attribution.

Attribution Problems

Attribution is essential for establishing state responsibility under international law. However, proxy warfare creates uncertainty regarding whether actions by armed groups may legally be attributed to sponsoring states. The International Court of Justice in *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States)* established the "effective control" test for attribution.¹³ Later, the International Criminal Tribunal for the Former Yugoslavia in *Prosecutor v Tadić* adopted the broader "overall control" standard.¹⁴ These differing standards continue to generate legal uncertainty in hybrid conflicts.

Threshold of Armed Conflict

Cyber-attacks and information operations further complicate classification. Not all hostile activities amount to armed conflicts under IHL. Consequently, determining when hybrid operations trigger the application of humanitarian law remains a contentious issue. Despite these challenges, most scholars argue that existing legal principles remain sufficiently flexible to regulate hybrid warfare, provided that factual circumstances satisfy established thresholds.

FUNDAMENTAL PRINCIPLES OF INTERNATIONAL HUMANITARIAN LAW IN CONTEMPORARY CONFLICT

Although warfare has evolved, the core principles of International Humanitarian Law remain unchanged.

1. Principle of Humanity

The principle of humanity seeks to minimize suffering and protect persons who are not participating in hostilities. Article 3 common to the Geneva Conventions prohibits:

- Murder;
- Torture;
- Cruel treatment;

¹² ICRC, How is the Term Armed Conflict Defined in International Humanitarian Law? <https://www.icrc.org/en/doc/assets/files/other/opinion-paper-armed-conflict.pdf>

¹³ *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States)*, ICJ Reports 1986 <https://www.icj-cij.org/case/70>

¹⁴ *Prosecutor v Dusko Tadić*, ICTY Appeals Chamber, 1999 <https://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf>

- Hostage-taking;
- Humiliating and degrading treatment.¹⁵

This principle remains relevant irrespective of the means and methods employed in hybrid warfare.

2. Principle of Distinction

Distinction is one of the cornerstones of IHL. Article 48 of Additional Protocol I requires parties to distinguish between:

- Civilians and combatants;
- Civilian objects and military objectives.¹⁶

Hybrid warfare complicates this principle because:

- Cyber operators may operate from civilian facilities;
- Non-state actors frequently blend with civilian populations;
- Social media platforms become instruments of information warfare;
- Critical infrastructure often serves both civilian and military functions.

The Israel-Hamas conflict and urban warfare in Gaza have demonstrated the difficulties associated with distinguishing military objectives from civilian infrastructure.¹⁷

3. Principle of Proportionality

Article 51(5)(b) of Additional Protocol I prohibits attacks likely to cause excessive civilian harm in relation to anticipated military advantage.¹⁸ In hybrid warfare, proportionality assessments become increasingly difficult because:

- Cyber operations may produce indirect effects;
- Dual-use infrastructure complicates targeting decisions;
- Civilian dependence on digital networks magnifies consequences.

Thus, commanders face unprecedented challenges when evaluating proportionality in cyberspace and densely populated urban environments.

4. Principle of Military Necessity

Military necessity permits only those measures necessary to achieve legitimate military objectives. However, military necessity does not justify violations of humanitarian law. The International Court of Justice emphasized in its Nuclear Weapons Advisory Opinion that humanitarian principles apply to all methods and means of warfare.¹⁹

¹⁵ Geneva Conventions, Common Article 3 <https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/article-3>

¹⁶ Additional Protocol I, Article 48 <https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-48>

¹⁷ ICRC, Urban Warfare and Protection of Civilians <https://www.icrc.org/en/urban-services-during-protracted-armed-conflict>

¹⁸ Additional Protocol I, Article 51(5)(b) <https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-51>

¹⁹ Legality of the Threat or Use of Nuclear Weapons, ICJ Advisory Opinion, 1996 <https://www.icj-cij.org/case/95>

5. Principle of Precaution

Article 57 of Additional Protocol I requires parties to take all feasible precautions to avoid civilian casualties.²⁰ Modern technologies, including artificial intelligence and precision-guided weapons, enhance precautionary capabilities. However, cyber warfare and information operations create uncertainties concerning indirect and cascading consequences.

CONTINUING RELEVANCE OF IHL PRINCIPLES

Despite technological transformations, these principles remain technologically neutral and adaptable. The International Committee of the Red Cross has repeatedly emphasized that the fundamental principles of humanity, distinction, proportionality, and precaution continue to govern all forms of armed conflict, including cyber operations and hybrid warfare.²¹ Therefore, the principal challenge is not the inadequacy of International Humanitarian Law itself but rather ensuring its effective interpretation and implementation within increasingly complex conflict environments.

Cyber Warfare and International Humanitarian Law

The increasing reliance on digital technologies has transformed cyberspace into an important domain of military operations. Cyber warfare refers to hostile activities conducted through computer networks with the intention of disrupting, degrading, manipulating, or destroying information systems and critical infrastructure. Modern military strategies increasingly incorporate cyber capabilities alongside conventional operations, making cyber warfare an integral component of hybrid conflict.

Unlike traditional kinetic attacks, cyber operations possess characteristics that complicate the application of International Humanitarian Law (IHL). Cyber-attacks may be launched remotely, attribution is often difficult, and the consequences may extend beyond national boundaries. Moreover, cyber operations can affect civilian infrastructure such as hospitals, power grids, transportation systems, banking networks, and communication systems without causing immediate physical destruction. The International Committee of the Red Cross (ICRC) maintains that existing principles of IHL apply equally to cyber operations conducted during armed conflict.²² Consequently, principles of distinction, proportionality, precaution, and military necessity remain applicable in cyberspace.

Distinction and Cyber Operations

Article 48 of Additional Protocol I requires parties to distinguish between civilian objects and military objectives.²³ However, modern information systems are frequently dual-use in nature. Communication networks, satellites, cloud computing infrastructure, and electrical grids often support both civilian and military functions. Consequently, distinguishing legitimate military targets from protected civilian infrastructure becomes increasingly difficult.

Proportionality and Incidental Harm

Cyber-attacks may produce indirect or cascading consequences. For example, an attack against electrical infrastructure could disrupt hospitals, transportation networks, and emergency services. Assessing whether

²⁰ Additional Protocol I, Article 57 <https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-57>

²¹ ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts (2024) <https://www.icrc.org/en/publication/international-humanitarian-law-and-challenges-contemporary-armed-conflicts-building>

²² Frank G Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars (Potomac Institute for Policy Studies 2007). https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

²³ Michael N Schmitt (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press 2017). <https://www.cambridge.org/core/books/tallinn-manual-20/9026B9E3F9A9C6B8A1E6C0B8E4F5A1F4>

expected civilian harm is excessive in relation to anticipated military advantage presents considerable legal challenges.

The Tallinn Manual

The Tallinn Manual on the International Law Applicable to Cyber Warfare represents one of the most influential scholarly attempts to clarify how existing international law applies to cyber operations. Although it does not possess binding legal authority, it provides persuasive guidance regarding state practice and legal interpretation.²⁴ The Manual concludes that cyber operations causing physical damage or injury may constitute attacks under IHL and are therefore subject to traditional humanitarian principles.

EMERGING CHALLENGES

Artificial intelligence, autonomous cyber capabilities, and quantum technologies further complicate legal regulation. The speed and unpredictability of cyber operations create uncertainties regarding accountability and proportionality assessments. Therefore, while existing law remains applicable, further clarification and international cooperation are necessary.

Information Warfare and Disinformation Campaigns

Information warfare constitutes another essential element of hybrid warfare. States and non-state actors increasingly employ propaganda, psychological operations, social media manipulation, and disinformation campaigns to influence public opinion and undermine adversaries. Unlike conventional military attacks, information operations often target cognitive and psychological domains. Their objectives include:

- Creating political instability;
- Influencing elections;
- Undermining confidence in institutions;
- Generating social polarization;
- Weakening enemy morale.

The Russia-Ukraine conflict has illustrated the strategic importance of information warfare. Both parties have extensively utilized social media platforms and digital communication to shape international narratives.²⁵

Applicability of IHL

International Humanitarian Law primarily regulates physical violence during armed conflict. Consequently, many forms of misinformation and propaganda fall outside its traditional scope. Nevertheless, information operations that incite genocide, war crimes, or violence against civilians may violate international law. Article 20 of the International Covenant on Civil and Political Rights prohibits advocacy of hatred constituting incitement to discrimination, hostility, or violence.²⁶ Similarly, international criminal tribunals have recognized that media propaganda may contribute to crimes against humanity and genocide. The International Criminal Tribunal for Rwanda in *Prosecutor v Nahimana* held that hate media played a significant role in facilitating genocide.²⁷ Therefore, while information warfare often falls within legal grey zones, international law imposes limits where propaganda directly contributes to international crimes.

²⁴ Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (3rd edn, CUP 2016). <https://www.cambridge.org/core/books/conduct-of-hostilities-under-the-law-of-international-armed-conflict/3A22D7A8F66C8DB66A2C7D7A5A3B2A65>

²⁵ Geneva Conventions of 1949. <https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949>

²⁶ Additional Protocol I (1977). <https://ihl-databases.icrc.org/en/ihl-treaties/api-1977>

²⁷ Additional Protocol II (1977). <https://ihl-databases.icrc.org/en/ihl-treaties/apii-1977>

Non-State Actors, Proxy Warfare, and Accountability

One of the defining characteristics of modern conflicts is the growing involvement of non-state actors. Terrorist organizations, insurgent groups, private military companies, and proxy militias have become central participants in contemporary warfare.

Examples include:

- Hamas;
- Hezbollah;
- Wagner Group;
- Houthis in Yemen;
- Islamic State (ISIS);
- Various armed factions operating in Syria and Libya.

These actors often operate across borders and maintain ambiguous relationships with states. Such relationships complicate the determination of legal responsibility.

Proxy Warfare

Proxy warfare allows states to pursue strategic objectives indirectly through allied armed groups. By employing proxies, states may avoid direct military confrontation and create uncertainty regarding attribution. The International Court of Justice in *Nicaragua v United States* established the "effective control" standard for attributing the actions of armed groups to states.²⁸ The International Criminal Tribunal for the Former Yugoslavia later developed the broader "overall control" test in *Tadić*.²⁹ The existence of different standards creates legal ambiguity concerning state responsibility in hybrid warfare.

Private Military Companies

Private military companies such as the Wagner Group have demonstrated the increasing privatization of armed conflict. Although individuals employed by such organizations remain bound by IHL, accountability mechanisms are often weak. Consequently, hybrid warfare raises significant questions regarding command responsibility, state responsibility, and individual criminal liability.

Case Study I: Russia–Ukraine Conflict

The Russia-Ukraine conflict represents one of the most prominent examples of hybrid warfare. Since 2014 and particularly after the full-scale invasion in February 2022, military operations have been accompanied by:

- Cyber-attacks;
- Economic sanctions;
- Information warfare;
- Disinformation campaigns;
- Drone warfare;

²⁸ International Covenant on Civil and Political Rights, 1966. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

²⁹ Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States) [1986] ICJ Rep 14. <https://www.icj-cij.org/case/70>

- Proxy activities;
- Use of private military companies.

The conflict demonstrates how kinetic operations are increasingly integrated with digital and informational dimensions. The International Criminal Court (ICC) issued arrest warrants against Russian President Vladimir Putin and Maria Lvova-Belova in March 2023 for alleged unlawful deportation of Ukrainian children.³⁰

The conflict has also generated extensive discussions regarding:

- Protection of civilians;
- Treatment of prisoners of war;
- Targeting of energy infrastructure;
- Accountability for war crimes.

The ICRC has emphasized that the Geneva Conventions apply fully to the conflict irrespective of its hybrid characteristics.³¹

Case Study II: Israel–Hammas Conflict

The Israel-Hamas conflict highlights the challenges posed by urban warfare and the participation of non-state actors. Following the attacks of 7 October 2023, hostilities escalated into large-scale military operations in Gaza. These operations have raised complex legal questions concerning:

- Distinction;
- Proportionality;
- Human shields;
- Hostage-taking;
- Protection of hospitals;
- Humanitarian access.

Urban warfare in densely populated areas increases the risk of civilian casualties and complicates compliance with IHL. The International Court of Justice, in *South Africa v Israel* (2024), issued provisional measures concerning obligations under the Genocide Convention.³² The conflict demonstrates how contemporary warfare involves not only military operations but also information campaigns, cyber dimensions, and international political pressures.

Challenges to Accountability and Enforcement

Despite universal ratification of the Geneva Conventions, enforcement remains one of the greatest weaknesses of International Humanitarian Law.

1. Attribution Problems

Hybrid warfare deliberately creates ambiguity and deniability, making it difficult to identify responsible actors.

2. Jurisdictional Limitations

International criminal tribunals possess limited jurisdiction and depend heavily on state cooperation.

³⁰ Prosecutor v. Dusko Tadić IT-94-1-A (ICTY Appeals Chamber, 15 July 1999). <https://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf>

³¹ Legality of the Threat or Use of Nuclear Weapons [1996] ICJ Rep 226. <https://www.icj-cij.org/case/95>

³² Prosecutor v. Nahimana et al. ICTR-99-52-A. <https://unictr.irmct.org/en/cases/ict9-99-52>

3. Political Constraints

The United Nations Security Council is frequently hindered by veto politics, limiting collective responses to violations.

4. Technological Developments

Artificial intelligence, autonomous weapons, and cyber capabilities evolve more rapidly than legal frameworks.

5. Non-State Actors

Many armed groups are unwilling to comply with humanitarian obligations, thereby undermining enforcement mechanisms. These challenges have led scholars to debate whether new treaties are required or whether existing legal principles should simply be interpreted more effectively.

Future of International Humanitarian Law in the Age of Hybrid Warfare

Most contemporary scholars and the International Committee of the Red Cross argue that existing IHL remains sufficiently flexible to regulate new forms of conflict.³³ However, certain areas require clarification:

Regulation of Cyber Operations

States should develop consensus regarding thresholds for cyber-attacks and protection of civilian infrastructure.

Artificial Intelligence and Autonomous Weapons

International negotiations are increasingly focused on ensuring meaningful human control over lethal autonomous systems.

Strengthening Accountability

Enhancing international criminal justice and improving mechanisms of state responsibility are essential.

Protection of Civilians

Urban warfare and digital technologies necessitate stronger safeguards for civilian populations.

International Cooperation

Greater cooperation among states, international organizations, and humanitarian institutions is necessary to ensure compliance.

Rather than replacing existing legal frameworks, the future development of IHL should focus on interpretation, implementation, and adaptation.

CONCLUSION

The changing character of armed conflict represents one of the most significant challenges confronting international law in the twenty-first century. Hybrid warfare has blurred traditional distinctions between war and peace, state and non-state actors, military and civilian domains, and physical and virtual battlefields. Cyber operations, disinformation campaigns, proxy warfare, and emerging technologies have transformed the conduct of hostilities and complicated the application of legal norms designed primarily for conventional interstate conflicts. Nevertheless, the fundamental principles of International Humanitarian Law—humanity, distinction, proportionality, military necessity, and precaution—remain technologically neutral and continue to provide an essential framework for regulating contemporary warfare. The Geneva Conventions and customary international law possess sufficient normative flexibility to govern many aspects of hybrid warfare. The principal difficulties lie not in the inadequacy of the law itself but in issues relating to classification, attribution, accountability, and enforcement.

³³ South Africa v Israel (Application of the Genocide Convention), ICJ (2024). <https://www.icj-cij.org/case/192>

Recent conflicts such as the Russia-Ukraine war and the Israel-Hamas conflict demonstrate that hybrid warfare creates unprecedented humanitarian consequences while simultaneously exposing weaknesses in international enforcement mechanisms. Cyber warfare, information operations, and proxy actors increasingly exploit legal grey areas, making effective regulation more difficult. Therefore, the future of International Humanitarian Law lies not in replacing existing norms but in strengthening their interpretation, enhancing international cooperation, improving accountability mechanisms, and adapting legal frameworks to technological realities. Preserving the humanitarian values embodied in IHL remains essential to ensuring that even in the age of hybrid warfare, the protection of human dignity continues to remain the cornerstone of international law.