Page 1806 - 1825

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 3

2026

Military Cyber Operations and the Crisis of Legal Accountability: Rethinking International Humanitarian Law in the Age of the Digital Battlespace

SHARAD KUMAR YADAV* AND DR. YUGDEEP KAUR**

ABSTRACT

Military cyber operations have emerged as a defining feature of contemporary conflict, transforming cyberspace into an operational domain where states can pursue strategic objectives without resorting to conventional armed force. The increasing reliance of governments, military institutions, and critical infrastructure on interconnected digital systems has expanded both the utility and the risks of cyber capabilities in matters of national security. While cyber operations offer significant strategic advantages, they have also exposed fundamental weaknesses in the existing legal framework governing armed conflict. International Humanitarian Law, developed primarily in the context of kinetic warfare, continues to provide important normative principles for regulating hostilities; however, its application to cyberspace remains uncertain in several respects. Questions relating to attribution, state responsibility, civilian protection, proportionality, and the involvement of non-state actors have generated a persistent crisis of legal accountability within the digital battlespace. This paper examines the extent to which existing international legal principles are capable of addressing the unique challenges posed by military cyber operations and evaluates the limitations of contemporary accountability mechanisms. It analyses the relevance of International Humanitarian Law, emerging international norms, and state practice in regulating cyber conflict while highlighting the practical difficulties associated with enforcing legal responsibility in an environment characterised by anonymity, technological complexity, and transnational effects. The paper argues that the central challenge in cyber warfare is not the complete absence of legal rules but the inadequacy of existing mechanisms for attributing responsibility and ensuring compliance. It concludes that strengthening accountability through clearer legal standards, enhanced international cooperation, and a human-centred approach to cyber governance is essential for preserving the legitimacy of international law and protecting humanitarian interests in an increasingly digitalised battlespace.

* Author is a Ph.D. Research Scholar at School of Law, Lovely Professional University, Punjab, India.
** Author is an Associate Professor (Law) at School of Law, Lovely Professional University, Punjab, India.

 [ISSN 2581-5369]

Keywords: *Military Cyber Operations; International Humanitarian Law; Legal Accountability; Cyber Warfare; Attribution in Cyberspace; Digital Battlespace.*

I. INTRODUCTION

The increasing dependence of states upon digital technologies has fundamentally transformed the nature of contemporary conflict. Cyberspace, once viewed primarily as a medium for communication and economic activity, has gradually evolved into an operational domain with significant military and strategic implications. Today, military cyber operations are capable of disrupting communication networks, compromising critical infrastructure, interfering with command-and-control systems, and influencing national security outcomes without the deployment of conventional armed forces. As governments continue to invest in offensive and defensive cyber capabilities, the digital battlespace has emerged as a central feature of modern warfare.[1]

Unlike traditional forms of armed conflict, military cyber operations frequently occur across territorial boundaries, are often conducted anonymously, and may produce consequences that are difficult to predict or attribute. Cyberattacks can target military installations, government institutions, financial networks, healthcare systems, and energy infrastructure, often through the same interconnected digital environment. The resulting convergence of civilian and military systems has created new challenges for international law, particularly in relation to accountability, civilian protection, and lawful state conduct during conflict.[2] While technological capabilities have advanced rapidly, the legal mechanisms governing their use have developed at a considerably slower pace.

International Humanitarian Law (IHL) remains the principal body of law regulating the conduct of hostilities during armed conflict. Built upon the principles of distinction, proportionality, military necessity, and humanity, IHL seeks to balance military objectives with the protection of civilian populations.[3] However, the application of these principles to cyberspace remains contested. Cyber operations rarely fit neatly within the conventional legal categories upon which humanitarian law was originally constructed. Difficulties relating to attribution, indirect effects, non-state actors, and transnational digital infrastructure have exposed significant

[1] P.W. Singer & Allan Friedman, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 95-103 (Oxford Univ. Press 2014).
[2] Marco Roscini, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 13-21 (Oxford Univ. Press 2014).
[3] Marco Sassòli, INTERNATIONAL HUMANITARIAN LAW: RULES, CONTROVERSIES AND SOLUTIONS TO PROBLEMS ARISING IN WARFARE 245-52 (Edward Elgar Publ'g 2019).

 [ISSN 2581-5369]

limitations in the existing regulatory framework. Consequently, although there is broad agreement that international law applies to cyberspace, considerable uncertainty persists regarding how accountability should be established when cyber operations cause harm.

The problem is particularly evident in relation to attribution. Unlike conventional military attacks, cyber operations are frequently designed to conceal the identity of those responsible. States may act through proxy groups, intelligence networks, or third-party digital infrastructure, making it difficult to determine whether a particular operation can be legally attributed to a state.[4] In the absence of reliable attribution, the enforcement of legal responsibility becomes increasingly complicated. This challenge is compounded by the fact that existing accountability mechanisms were developed primarily for kinetic warfare and often struggle to accommodate the technical realities of cyberspace.

Existing scholarship has extensively examined issues such as cyber warfare, cyber sovereignty, and the applicability of international law to cyber operations. However, comparatively limited attention has been devoted to the broader crisis of legal accountability that emerges when military cyber activities cannot be effectively attributed, investigated, or regulated. Much of the contemporary debate focuses upon whether cyber operations constitute a use of force or an armed attack, while questions concerning accountability and enforcement frequently receive less systematic analysis. This paper seeks to address that gap by examining how existing principles of International Humanitarian Law respond to accountability challenges arising within the digital battlespace.

The central objective of this study is to evaluate the adequacy of current legal frameworks in regulating military cyber operations and ensuring accountability for unlawful conduct in cyberspace. It examines the applicability of International Humanitarian Law to cyber conflict, analyses the challenges posed by attribution and state responsibility, and assesses emerging international efforts aimed at strengthening legal governance in cyberspace. The study further explores whether existing legal principles remain sufficient in the face of evolving technological realities or whether a rethinking of accountability mechanisms has become necessary.

Methodologically, the paper adopts a doctrinal and analytical approach based primarily upon international legal instruments, judicial and quasi-judicial materials, scholarly literature, and institutional reports. Particular attention is given to the United Nations Charter, the Geneva Conventions and their Additional Protocols, the Tallinn Manual 2.0, and relevant developments

[4] Kristen Eichensehr, *The Law & Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520, 525-33 (2020).

 [ISSN 2581-5369]

within international cyber governance. Comparative reference is also made to emerging state practice and international norm-building initiatives where relevant.

The paper is divided into six substantive parts. Following this Introduction, Part II examines the concept and contemporary relevance of military cyber operations. Part III analyses the applicability of International Humanitarian Law to cyber warfare. Part IV explores the accountability crisis arising from attribution difficulties and limitations of state responsibility. Part V evaluates emerging international legal responses and normative developments. Part VI proposes a framework for strengthening accountability in the digital battlespace. The paper concludes by arguing that while existing legal principles continue to provide an important foundation for regulating cyber conflict, meaningful accountability requires clearer standards, stronger international cooperation, and renewed attention to the protection of humanitarian values within cyberspace.

II. MILITARY CYBER OPERATIONS: CONCEPT AND CONTEMPORARY RELEVANCE

Military cyber operations have emerged as an integral component of contemporary national security strategy. States increasingly rely upon cyber capabilities to gather intelligence, disrupt adversarial networks, protect critical infrastructure, and achieve strategic objectives without engaging in conventional military confrontation. Unlike traditional forms of warfare, cyber operations are conducted through digital systems and networked infrastructure, enabling states to project power across territorial boundaries with speed, precision, and a comparatively low risk of immediate escalation.[5] The growing strategic value of cyberspace has led many governments to recognise it as an operational domain alongside land, sea, air, and outer space.

Although the term "cyber warfare" is frequently used in political and academic discourse, military cyber operations encompass a broader range of activities than armed conflict alone. Such operations may include cyber espionage, network exploitation, disruption of communication systems, interference with critical infrastructure, and offensive actions directed against military targets.[6] Not all cyber activities constitute warfare in the legal sense; however, they increasingly form part of military planning and strategic competition between states. Consequently, understanding the nature of military cyber operations is essential for evaluating the legal challenges associated with accountability and regulation.

A useful distinction must be drawn between cybercrime and military cyber operations. Cybercrime is generally motivated by financial gain, personal objectives, or criminal intent and

[5] P.W. Singer & Allan Friedman, *supra* note 1, at 95-103.
[6] Michael N. Schmitt, *Cyber Operations and the Jus ad Bellum Revisited*, 56 VILL. L. REV. 569, 571-76 (2011).

 [ISSN 2581-5369]

is regulated primarily through domestic criminal law. Military cyber operations, by contrast, are undertaken in pursuit of strategic, political, or security objectives and often involve state actors or entities acting on behalf of states.[7] This distinction is important because the legal frameworks governing criminal conduct differ significantly from those applicable to interstate conflict and the law of armed conflict.

Military cyber operations may broadly be categorised as defensive or offensive. Defensive cyber operations focus on protecting military and governmental networks from intrusion, disruption, or sabotage. They include activities such as threat detection, network security, incident response, and resilience-building measures. Offensive cyber operations, on the other hand, are designed to achieve strategic effects within adversarial systems through disruption, degradation, manipulation, or destruction of digital infrastructure.[8] In practice, however, the distinction between offensive and defensive activities is often blurred, particularly where states engage in proactive measures intended to neutralise threats before they materialise.

The increasing prominence of cyber operations reflects a broader transformation in the nature of warfare. Contemporary conflicts are no longer confined to physical battlefields but increasingly involve digital environments where information, communication, and infrastructure become targets of strategic significance. The 2007 cyberattacks against Estonia and the Stuxnet operation targeting Iranian nuclear facilities demonstrated that cyber capabilities can produce consequences with substantial political, economic, and security implications.[9] These incidents reinforced the view that cyberspace is not merely a technological environment but a domain capable of influencing national power and international stability.

At the same time, military cyber operations present characteristics that distinguish them from conventional forms of warfare. One of the most significant features is the difficulty of attribution. Cyber operations can be conducted through anonymised networks, proxy actors, or compromised third-party systems, making it difficult to identify the responsible actor with certainty.[10] This challenge has profound legal implications because accountability under international law depends heavily upon establishing responsibility for wrongful conduct.

Another distinctive characteristic is the interconnected nature of modern digital infrastructure. Military and civilian systems frequently rely upon shared networks and technological platforms.

[7] Thomas Rid, CYBER WAR WILL NOT TAKE PLACE 1-15 (Oxford Univ. Press 2013).
[8] U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE CYBER STRATEGY 1-5 (2018).
[9] Eneken Tikk, Kadri Kaska & Liis Vihul, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 14-22 (NATO Cooperative Cyber Defence Centre of Excellence 2010); Ralph Langner, *Stuxnet: Dissecting a Cyberwarfare Weapon*, 9 IEEE SEC. & PRIV. 49, 49-51 (2011).
[10] Eichensehr, *supra* note 4, at 525-33.

 [ISSN 2581-5369]

As a result, cyber operations directed at military objectives may inadvertently affect civilian services such as healthcare, banking, transportation, or energy distribution.[11] This interconnectedness complicates the application of traditional legal principles governing armed conflict and raises concerns regarding civilian protection within cyberspace.

The strategic significance of military cyber operations is further reflected in the growing institutionalisation of cyber capabilities. Several states have established dedicated cyber commands and specialised units responsible for offensive and defensive cyber activities. The United States Cyber Command, the United Kingdom's National Cyber Force, and comparable institutions in other jurisdictions illustrate the increasing integration of cyber capabilities into military doctrine and national security policy.[12] These developments demonstrate that cyber operations are no longer peripheral instruments of statecraft but central components of contemporary military strategy.

The emergence of the digital battlespace therefore represents more than a technological development; it reflects a fundamental shift in the methods through which states pursue security and strategic advantage. Yet, while military cyber capabilities have expanded rapidly, the legal framework governing their use remains comparatively underdeveloped. Questions concerning accountability, attribution, state responsibility, and humanitarian protection continue to generate uncertainty within international law. Understanding the nature and contemporary relevance of military cyber operations is therefore a necessary first step in examining the broader crisis of legal accountability that characterises modern cyber conflict.

III. INTERNATIONAL HUMANITARIAN LAW AND CYBER WARFARE

The increasing use of cyber capabilities in military operations has generated an important legal question: whether the existing framework of International Humanitarian Law (IHL) is capable of regulating conduct within the digital battlespace. Although the Geneva Conventions and their Additional Protocols were drafted long before the emergence of cyberspace as a domain of conflict, there is broad consensus among states, international organisations, and legal scholars that IHL applies to cyber operations conducted during armed conflict.[13] The principal challenge is therefore not the applicability of IHL itself, but the manner in which its traditional principles should be interpreted and enforced in a technologically complex environment.

[11] Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 379-83 (2011).
[12] Max Smeets, NO SHORTCUTS: WHY STATES STRUGGLE TO DEVELOP A MILITARY CYBER-FORCE 88-96 (Oxford Univ. Press 2022).
[13] INT'L COMM. OF THE RED CROSS, INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICTS 42-45 (2019).

 [ISSN 2581-5369]

At its core, IHL seeks to limit the effects of armed conflict by balancing military necessity with humanitarian considerations. The principles of distinction, proportionality, and military necessity remain central to this objective and continue to provide the primary legal framework for assessing the legality of military cyber operations.[14] However, applying these principles to cyber activities often proves considerably more difficult than in conventional warfare.

The principle of distinction requires parties to an armed conflict to differentiate between military objectives and civilian persons or objects.[15] In conventional warfare, identifying military targets is often linked to physical infrastructure, combat personnel, or military installations. In cyberspace, however, military and civilian systems are frequently interconnected. Communication networks, cloud services, satellite infrastructure, and digital platforms may simultaneously support civilian activities and military functions. As a result, cyber operations directed at legitimate military objectives may inadvertently affect civilian systems, thereby complicating compliance with the principle of distinction.[16]

Closely related is the principle of proportionality, which prohibits attacks expected to cause incidental civilian harm excessive in relation to the anticipated military advantage.[17] The assessment of proportionality becomes particularly challenging in cyberspace because the consequences of cyber operations are often indirect, unpredictable, and capable of spreading across interconnected networks. A cyber operation designed to disable a military communication system may also disrupt civilian services such as healthcare, transportation, or financial infrastructure.[18] Determining the foreseeable scale of such effects before an operation is launched remains a significant legal and operational challenge.

The principle of military necessity similarly requires careful consideration within cyber conflict. Under IHL, military force may only be employed to the extent necessary to achieve a legitimate military objective.[19] While cyber capabilities may offer less destructive alternatives to conventional weapons, they may also create long-term or unintended consequences that are difficult to assess in advance. The absence of physical destruction does not necessarily eliminate

[14] Sassòli, *supra* note 3, at 245-52.
[15] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 48, June 8, 1977, 1125 U.N.T.S. 3.
[16] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 415-21 (Michael N. Schmitt ed., Cambridge Univ. Press 2017).
[17] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 51(5)(b), June 8, 1977, 1125 U.N.T.S. 3.
[18] Hollis, *supra* note 11, at 381-86.
[19] Yoram Dinstein, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 18-22 (3d ed. 2016).

 [ISSN 2581-5369]

humanitarian concerns where essential civilian services are affected or where digital disruption produces substantial societal harm.

Another issue concerns the protection of civilian infrastructure. Modern societies depend heavily upon digital systems for the delivery of essential services, including healthcare, energy distribution, banking, transportation, and emergency communications. Cyber operations targeting or affecting such systems may create humanitarian consequences comparable to those associated with conventional attacks.[20] The International Committee of the Red Cross has therefore emphasised that existing humanitarian protections must remain applicable regardless of the technological means employed during conflict.[21]

The Tallinn Manual 2.0 has played an important role in clarifying how existing international law may apply to cyber operations. Although it does not constitute binding law, the Manual reflects extensive expert analysis concerning the interaction between cyberspace and established legal principles.[22] It supports the view that cyber operations conducted during armed conflict remain subject to the rules of distinction, proportionality, necessity, and humanity. Nevertheless, the Manual also highlights areas of continuing disagreement, particularly regarding sovereignty, attribution, and the threshold at which cyber operations amount to attacks under international law.

Despite these interpretative efforts, significant uncertainty persists. The technical complexity of cyber operations, the difficulty of identifying responsible actors, and the interconnected nature of digital infrastructure frequently hinder effective enforcement of humanitarian obligations. Consequently, while International Humanitarian Law continues to provide an essential normative framework, its practical application within cyberspace remains imperfect and often dependent upon evolving state practice and scholarly interpretation.

The relevance of IHL to cyber warfare is therefore beyond serious dispute; however, its effectiveness increasingly depends upon the ability of the international legal system to adapt traditional principles to new technological realities. This challenge becomes most apparent when questions of attribution and responsibility arise, for it is at this point that the broader crisis of legal accountability within the digital battlespace begins to emerge.

A. Jus ad Bellum and Jus in Bello in Cyberspace

[20] Roscini, *supra* note 2, at 187-93.
[21] INT'L COMM. OF THE RED CROSS, AVOIDING CIVILIAN HARM FROM MILITARY CYBER OPERATIONS DURING ARMED CONFLICTS 3-7 (2021).
[22] TALLINN MANUAL 2.0, *supra* note 16, at 3-11.

 [ISSN 2581-5369]

The legal regulation of military cyber operations is generally examined through two complementary branches of international law: *jus ad bellum* and *jus in bello*. While *jus ad bellum* governs the legality of resorting to force, *jus in bello* regulates the conduct of hostilities once an armed conflict exists.[23] Together, these principles form the normative foundation upon which contemporary debates concerning cyber warfare and legal accountability are constructed.

In the cyber context, *jus ad bellum* raises the question of whether a cyber operation may amount to a prohibited use of force or an armed attack under the United Nations Charter. Article 2(4) prohibits the threat or use of force against the territorial integrity or political independence of any state, while Article 51 recognises the inherent right of self-defence in response to an armed attack.[24] The difficulty, however, lies in determining when a cyber operation crosses the threshold from espionage, disruption, or interference into an act capable of triggering legal consequences under the Charter framework. Unlike conventional military attacks, cyber operations often produce indirect effects and may not result in immediate physical destruction, thereby complicating the assessment of force and self-defence.[25]

The Stuxnet operation against Iran's Natanz nuclear facility illustrates this dilemma. Although the malware reportedly caused physical damage to uranium-enrichment centrifuges, the operation occurred through digital means and without conventional military engagement.[26] The incident generated significant scholarly debate regarding whether cyber operations producing kinetic consequences should be treated similarly to traditional armed attacks under *jus ad bellum*. Similar questions continue to arise in the context of cyber activities associated with geopolitical tensions involving states such as Iran, Israel, Russia, Ukraine, and the United States.

Once an armed conflict exists, *jus in bello* becomes the primary legal framework governing cyber operations. This body of law seeks to minimise unnecessary suffering and protect civilians by regulating the methods and means of warfare.[27] The principles of distinction, proportionality, military necessity, and humanity apply irrespective of the technology employed during hostilities. Consequently, cyber operations conducted during armed conflict must comply with the same humanitarian obligations that govern conventional military action.

[23] Yoram Dinstein, WAR, AGGRESSION AND SELF-DEFENCE 87-93 (6th ed. 2017).
[24] U.N. Charter arts. 2(4), 51.
[25] Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 914-18 (1999).
[26] Langner, *supra* note 9, at 49-51.
[27] Sassòli, *supra* note 3, at 245-52.

 [ISSN 2581-5369]

The application of *jus in bello* to cyberspace nevertheless presents unique challenges. Military and civilian systems frequently operate through interconnected digital networks, making it difficult to distinguish legitimate military objectives from civilian infrastructure.[28] Moreover, the effects of cyber operations may be unpredictable and capable of spreading beyond intended targets. These characteristics complicate the implementation of traditional humanitarian safeguards and expose gaps in existing accountability mechanisms.

Although significant disagreement remains regarding the precise application of these doctrines in cyberspace, *jus ad bellum* and *jus in bello* continue to provide the principal legal framework through which the legality of military cyber operations is assessed. Their relevance demonstrates that cyberspace exists neither beyond the reach of international law nor outside established humanitarian principles. Rather, the contemporary challenge lies in adapting these long-standing legal doctrines to a battlespace defined by anonymity, interconnectedness, and technological complexity.

B. Principle of Distinction

The principle of distinction constitutes a cornerstone of International Humanitarian Law and requires parties to an armed conflict to distinguish between military objectives and civilian persons or objects.[29] Cyber warfare complicates this obligation because military and civilian systems frequently rely upon shared digital infrastructure. Communication networks, cloud services, financial systems, and satellite technologies often perform both civilian and military functions simultaneously.[30] As a result, cyber operations directed against legitimate military objectives may inadvertently affect civilian infrastructure and essential public services.

The challenge is particularly evident where cyber operations target dual-use systems. Unlike conventional military targets, digital infrastructure is rarely segregated according to civilian or military use. Consequently, ensuring compliance with the principle of distinction requires heightened caution and careful target assessment. The difficulty of applying this principle within cyberspace reflects one of the broader accountability challenges facing contemporary military cyber operations.

C. Principle of Proportionality

The principle of proportionality prohibits attacks expected to cause incidental civilian harm that would be excessive in relation to the anticipated military advantage.[31] In conventional warfare,

[28] TALLINN MANUAL 2.0, *supra* note 16, at 415-21.
[29] Protocol Additional to the Geneva Conventions, *supra* note 15, art. 48.
[30] TALLINN MANUAL 2.0, *supra* note 16, at 415-21.
[31] Protocol Additional to the Geneva Conventions, *supra* note 17, art. 51(5)(b).

 [ISSN 2581-5369]

proportionality assessments generally focus upon foreseeable physical damage and civilian casualties. Cyber operations, however, often produce indirect and interconnected consequences that are difficult to predict in advance.

A cyber operation targeting a military communication system may unintentionally disrupt hospitals, transportation networks, banking services, or energy infrastructure. Such cascading effects complicate the assessment of civilian harm and make proportionality evaluations significantly more challenging.[32] The legal uncertainty surrounding these consequences further contributes to the accountability deficit in cyberspace, as states may struggle to determine whether a cyber operation complied with humanitarian obligations at the time it was conducted.

D. Principle of Military Necessity

The principle of military necessity permits the use of force only to the extent required to achieve a legitimate military objective.[33] The principle seeks to balance operational effectiveness with humanitarian restraint by prohibiting actions that do not contribute directly to military success.

In the cyber domain, military necessity assumes particular importance because cyber capabilities are often presented as less destructive alternatives to conventional weapons.[34] Nevertheless, the absence of physical violence does not automatically render a cyber operation lawful. Where a cyber activity causes widespread disruption to civilian systems without producing a concrete military advantage, its legality may be questioned under the doctrine of military necessity. Consequently, military cyber operations must be evaluated not only according to their effectiveness but also according to their necessity within the broader context of armed conflict.

E. Protection of Civilian Infrastructure

The protection of civilian infrastructure has become one of the most pressing humanitarian concerns in contemporary cyber conflict. Modern societies depend heavily upon digital systems for healthcare, electricity, water supply, banking, transportation, and emergency communication. Cyber operations affecting these systems may generate severe humanitarian consequences even in the absence of physical destruction.[35]

The increasing interdependence between civilian and military networks creates additional risks. A cyber operation directed at military objectives may unintentionally compromise services

[32] Sassòli, *supra* note 3, at 248-52.
[33] Dinstein, *supra* note 19, at 18-22.
[34] Nils Melzer, CYBERWARFARE AND INTERNATIONAL LAW 18-22 (U.N. Inst. for Disarmament Rsch. 2011).
[35] Int'l Comm. of the Red Cross, *supra* note 21, at 3-7.

 [ISSN 2581-5369]

relied upon by civilians, thereby undermining humanitarian protections embedded within International Humanitarian Law.[36] The International Committee of the Red Cross has repeatedly emphasised that civilian infrastructure should not become an indirect casualty of cyber warfare. Accordingly, effective accountability mechanisms must include safeguards designed to minimise civilian harm and ensure compliance with humanitarian obligations in the digital battlespace.

IV. THE ACCOUNTABILITY CRISIS IN MILITARY CYBER OPERATIONS

While International Humanitarian Law provides a normative framework for regulating conduct during armed conflict, its effectiveness depends upon the ability to identify violations and assign responsibility to the actors involved. In conventional warfare, accountability is generally linked to identifiable military forces, territorial operations, and observable consequences. Cyber operations, however, challenge these assumptions by operating through anonymous networks, transnational infrastructure, and technologically sophisticated methods designed to conceal the identity of those responsible. As a result, the most significant legal challenge posed by military cyber operations is not the absence of applicable law but the difficulty of enforcing accountability within the digital battlespace.[37]

The problem begins with attribution. Under international law, a state may be held responsible for internationally wrongful acts only when the conduct in question can be attributed to it.[38] In cyberspace, establishing attribution is exceptionally difficult. Cyber operations are frequently routed through multiple jurisdictions, compromised systems, and proxy networks that obscure their origin. Even where technical indicators suggest the involvement of a particular actor, such evidence may not satisfy the legal or political threshold required for international responsibility.[39] Consequently, states often encounter significant obstacles when attempting to identify perpetrators with sufficient certainty.

The attribution problem becomes more complex when states rely upon non-state actors, private groups, or proxy organisations to conduct cyber operations. Unlike conventional military forces, these actors may operate without formal affiliation while still advancing strategic objectives aligned with state interests. International law recognises that conduct may be attributed to a

[36] Hollis, *supra* note 11, at 381-86.
[37] Schmitt, *supra* note 6, at 580-84.
[38] Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts art. 2, U.N. Doc. A/56/10 (2001).
[39] Eichensehr, *supra* note 4, at 525-33.

 [ISSN 2581-5369]

state where it exercises effective control over the actors concerned.[40] However, demonstrating such control in cyberspace is often difficult because evidence regarding operational direction, financing, or coordination is rarely publicly available. This creates opportunities for states to benefit from plausible deniability while avoiding direct legal responsibility.

The challenge of attribution directly affects the operation of the law of state responsibility. The Articles on Responsibility of States for Internationally Wrongful Acts provide a general framework for assigning responsibility when a state breaches an international obligation.[41] Yet the practical effectiveness of these principles depends upon the ability to establish both attribution and a violation of international law. In the cyber context, uncertainty surrounding attribution frequently prevents the application of these rules, thereby limiting their deterrent effect and weakening accountability mechanisms.

Another dimension of the accountability crisis concerns enforcement. International law lacks a centralised enforcement authority capable of investigating and adjudicating cyber incidents in a consistent manner. Responses to major cyber operations are therefore often shaped by political considerations rather than formal legal processes.[42] States may impose sanctions, pursue diplomatic measures, or engage in countermeasures, but such responses frequently occur outside traditional judicial mechanisms. As a result, accountability for cyber operations often remains fragmented and inconsistent.

The difficulties associated with accountability are particularly evident in relation to cyber operations that fall below the threshold of armed attack. Many military cyber activities involve espionage, network intrusion, data manipulation, or disruption of services rather than large-scale physical destruction.[43] Although such activities may cause significant strategic harm, they often occupy a legal grey area in which existing rules provide limited guidance regarding responsibility and permissible responses. This ambiguity encourages strategic behaviour designed to exploit legal uncertainty while avoiding clear violations of international law.

The emergence of artificial intelligence and increasingly autonomous cyber capabilities introduces further complications. As cyber operations become more automated, questions arise regarding responsibility for unintended consequences resulting from algorithmic decision-

[40] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 115 (June 27).
[41] Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 38, arts. 4-11.
[42] Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1031-36 (2007).
[43] Rid, *supra* note 7, at 9-15.

 [ISSN 2581-5369]

making. Where an autonomous system identifies targets, exploits vulnerabilities, or causes unforeseen harm, determining who bears legal responsibility becomes considerably more difficult.[44] Existing legal frameworks were developed on the assumption that human actors make operational decisions; they are less equipped to address scenarios involving significant machine autonomy.

The accountability crisis therefore reflects a broader mismatch between technological capability and legal governance. Military cyber operations are increasingly capable of producing strategic effects comparable to those associated with traditional military action, yet mechanisms for assigning responsibility remain uncertain and fragmented. Without effective attribution, reliable investigative processes, and clearer standards of responsibility, the deterrent and regulatory functions of international law risk being weakened.

Ultimately, the challenge facing contemporary international law is not whether cyber operations should be regulated, but how accountability can be maintained in an environment where identifying responsible actors is often the most difficult aspect of the conflict itself. Addressing this challenge is essential if legal norms governing armed conflict are to remain relevant and effective within the digital battlespace.

F. Illustrating the Accountability Crisis: Lessons from Contemporary Cyber Conflicts

The practical consequences of the accountability deficit become apparent when examining major cyber incidents of the last two decades. One of the most frequently cited examples is the **Stuxnet operation**, which targeted Iran's Natanz nuclear facility and reportedly caused physical damage to uranium-enrichment centrifuges. Although the operation is widely attributed to the United States and Israel, neither state formally accepted responsibility.[45] The incident demonstrated that cyber operations can achieve strategic military objectives traditionally associated with conventional force while simultaneously complicating questions of attribution and legal accountability.

The continuing cyber confrontation between Israel and Iran further illustrates these difficulties. Over the past decade, both states have been linked to cyber operations targeting governmental systems, critical infrastructure, financial institutions, and communication networks. More recently, cyber activities accompanying periods of military escalation have included attacks

[44] Heather M. Roff & Richard Moyes, *Meaningful Human Control, Artificial Intelligence and Autonomous Weapons* 4-9 (Article 36, 2016).
[45] Langner, *supra* note 9, at 49-51.

 [ISSN 2581-5369]

against banking services, public infrastructure, and information systems.[46] Yet despite extensive public reporting and technical attribution by cybersecurity researchers, formal legal accountability has remained largely absent. The recurring reliance on proxy actors, hacker collectives, and unofficial groups enables states to benefit from plausible deniability while avoiding direct legal consequences.[47]

The 2007 cyberattacks against Estonia provide another important example. The attacks disrupted government websites, banking services, media organisations, and communication networks following a diplomatic dispute with Russia. Although substantial evidence suggested Russian involvement or support from actors operating within Russian territory, definitive legal attribution proved difficult.[48] The incident exposed the limitations of existing international law when dealing with large-scale cyber disruptions that produce significant national consequences without clear identification of the responsible state.

Similar concerns emerged in relation to the **NotPetya malware** attack of 2017. Originally directed at Ukrainian targets, the malware rapidly spread across international networks, causing billions of dollars in economic losses worldwide. Several governments publicly attributed the operation to actors associated with the Russian Federation; however, translating political attribution into enforceable legal responsibility remained considerably more challenging.[49] The incident highlighted how cyber operations can generate transnational consequences far beyond their intended targets while existing accountability mechanisms struggle to provide effective remedies.

Even where cyber operations are linked to broader military or political campaigns, questions of responsibility often remain unresolved. Allegations concerning cyber interference in Venezuelan infrastructure, including claims that cyber capabilities may have contributed to disruptions affecting critical services, illustrate how difficult it remains to distinguish between political accusation, technical attribution, and legally verifiable responsibility.[50] Such cases demonstrate that the accountability challenge is not limited to identifying perpetrators; it also involves establishing evidentiary standards capable of supporting lawful international responses.

---

[46] See CTR. FOR STRATEGIC & INT'L STUD., *How Will Cyber Warfare Shape the U.S.-Israel Conflict with Iran?* (Mar. 9, 2026).
[47] *Id.*
[48] Tikk, Kaska & Vihul, *supra* note 9, at 14-22.
[49] Press Release, U.S. DEP'T OF JUSTICE, *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace* (Oct. 19, 2020).
[50] See CTR. FOR STRATEGIC & INT'L STUD., *Iran Conflict Heightens Cyber Threats to U.S. Energy Infrastructure* (2026).

 [ISSN 2581-5369]

Taken together, these incidents reveal a recurring pattern. Technical attribution may be possible, political attribution may be asserted, yet legal accountability frequently remains elusive. This gap between identifying likely perpetrators and establishing internationally recognised responsibility constitutes the central accountability crisis confronting contemporary military cyber operations.

V. INTERNATIONAL LEGAL RESPONSES AND EMERGING NORMS

The growing strategic significance of cyberspace has prompted increasing efforts at the international level to develop legal and normative frameworks capable of regulating state conduct in the digital domain. While no comprehensive treaty governing military cyber operations currently exists, several international initiatives have sought to clarify the applicability of existing international law and promote responsible behaviour in cyberspace. These developments represent important steps towards accountability; however, significant gaps remain in their practical implementation.

One of the most influential contributions to contemporary cyber law discourse is the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Developed by an international group of legal experts under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence, the Manual seeks to explain how existing international law applies to cyber activities.[51] Although it does not possess binding legal authority, the Manual has become a widely cited reference in discussions concerning sovereignty, use of force, self-defence, state responsibility, and humanitarian obligations in cyberspace. Importantly, it reinforces the view that cyber operations are not beyond the reach of international law merely because they occur through digital means.

Despite its significance, the Tallinn Manual has notable limitations. It reflects expert interpretation rather than state consensus and therefore cannot create new legal obligations.[52] Several states have adopted differing positions regarding issues such as sovereignty, countermeasures, and the threshold at which cyber operations amount to a use of force. As a result, the Manual provides guidance but does not eliminate legal uncertainty.

At the multilateral level, the United Nations has played an increasingly important role in cyber governance. The United Nations Group of Governmental Experts (UN GGE) has repeatedly affirmed that existing international law, including the United Nations Charter, applies to state

[51] TALLINN MANUAL 2.0, *supra* note 16, at 3-11.
[52] Nicholas Tsagourias & Russell Buchan, RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 35-42 (Edward Elgar Publ'g 2015).

 [ISSN 2581-5369]

conduct in cyberspace.[53] Similarly, the Open-Ended Working Group (OEWG) has sought to encourage dialogue among states concerning responsible behaviour, confidence-building measures, and the prevention of conflict in the digital environment.[54] These initiatives have contributed to the gradual development of normative expectations regarding state conduct.

However, the effectiveness of these processes remains limited by the absence of binding enforcement mechanisms. International consensus often exists at a general level, particularly regarding the applicability of international law, yet substantial disagreement persists concerning specific questions of attribution, self-defence, countermeasures, and state responsibility.[55] Consequently, states frequently interpret legal obligations in ways that align with their strategic interests, resulting in divergent approaches to cyber governance.

State practice has also contributed to the gradual emergence of norms governing cyber operations. Public attribution statements issued by states following incidents such as the SolarWinds compromise, the NotPetya malware attack, and cyber operations associated with geopolitical tensions involving Russia, Iran, and North Korea demonstrate a growing willingness to identify and condemn malicious cyber activities.[56] Nevertheless, public attribution alone does not necessarily translate into legal accountability. Political attribution may influence international opinion, but it often falls short of establishing enforceable responsibility under international law.

The emergence of these initiatives demonstrates that cyberspace is gradually moving towards a more structured legal environment. Yet the central problem identified in this paper remains unresolved. Existing frameworks help clarify legal principles, encourage responsible behaviour, and promote international dialogue, but they do not fully address the practical difficulties associated with attribution, enforcement, and accountability. The result is a regulatory landscape in which legal norms exist, but mechanisms for ensuring compliance remain comparatively weak.[57]

Accordingly, while contemporary international initiatives represent important progress, they should be viewed as transitional rather than comprehensive solutions. The future effectiveness of cyber governance will depend upon the development of stronger accountability mechanisms

[53] U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/70/174 (July 22, 2015).
[54] U.N. Secretary-General, *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/75/816 (Mar. 18, 2021).
[55] Schmitt, *supra* note 6, at 580-84.
[56] Eichensehr, *supra* note 4, at 548-56.
[57] Eichensehr, *supra* note 4, at 525-33.

 [ISSN 2581-5369]

capable of bridging the gap between legal principle and practical enforcement within the digital battlespace.

VI. Rethinking Accountability in the Digital Battlespace

The preceding discussion demonstrates that the principal challenge confronting the regulation of military cyber operations is not the absence of applicable legal norms but the inadequacy of existing mechanisms for ensuring accountability. International Humanitarian Law, the law of state responsibility, and the broader framework of international law continue to provide important normative standards. Yet the practical difficulties associated with attribution, enforcement, and technological complexity frequently prevent these standards from operating effectively. Addressing the accountability crisis therefore requires a shift from merely recognising legal obligations to strengthening the mechanisms through which those obligations are implemented and enforced.

A first priority is the development of clearer international standards concerning attribution. While technical attribution is primarily a matter of cybersecurity expertise, legal accountability depends upon the existence of broadly accepted evidentiary standards capable of supporting international responsibility.[58] At present, states often apply differing thresholds when publicly attributing cyber operations to foreign actors. Greater convergence regarding evidentiary requirements would reduce uncertainty and enhance the legitimacy of international responses to malicious cyber activities. Such standards need not eliminate all ambiguity; rather, they should provide a sufficiently reliable basis for diplomatic, legal, and institutional action.

A second area requiring attention is the strengthening of state responsibility in cyberspace. Existing principles contained in the Articles on Responsibility of States for Internationally Wrongful Acts remain applicable to cyber operations, yet their practical enforcement remains limited.[59] States should increasingly recognise that responsibility may arise not only from direct participation in cyber operations but also from knowingly permitting their territory, infrastructure, or resources to be used for internationally wrongful cyber activities. Greater emphasis upon due diligence obligations could contribute to a more accountable cyber environment while discouraging the use of proxy actors and indirect methods of cyber aggression.

[58] Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 38, arts. 2, 4-11.
[59] Int'l Comm. of the Red Cross, *supra* note 21, at 3-7.

 [ISSN 2581-5369]

The protection of civilian digital infrastructure should also become a central objective of future cyber governance. Modern societies depend upon interconnected systems that support healthcare, transportation, banking, energy distribution, and emergency services. Cyber operations affecting such infrastructure may generate humanitarian consequences comparable to those associated with conventional military attacks.[60] Accordingly, states should work towards developing clearer norms concerning the protection of critical civilian infrastructure during both peacetime and armed conflict. Strengthening these protections would reinforce the humanitarian foundations of International Humanitarian Law while reducing risks to civilian populations.

The growing integration of artificial intelligence into military cyber capabilities further underscores the need for human-centred accountability mechanisms. Autonomous and semi-autonomous systems may enhance operational efficiency, but they also complicate traditional assumptions regarding legal responsibility and decision-making.[61] Meaningful human oversight should therefore remain a guiding principle in the development and deployment of military cyber technologies. Retaining human involvement in decisions capable of producing significant legal or humanitarian consequences is essential for preserving accountability and preventing responsibility from becoming diffused across complex technological systems.

International cooperation remains equally important. Cyber operations frequently transcend national borders, making purely domestic responses insufficient. Existing initiatives within the United Nations, including the UN GGE and OEWG processes, provide valuable forums for dialogue and norm development. However, greater emphasis should be placed upon information sharing, confidence-building measures, incident reporting, and cooperative attribution mechanisms. Such initiatives may not eliminate cyber conflict, but they can contribute to transparency and reduce the risk of escalation arising from uncertainty or miscalculation.

Ultimately, rethinking accountability in the digital battlespace requires recognising that cyber warfare presents challenges fundamentally different from those associated with conventional armed conflict. Legal frameworks designed for a world of identifiable armies and geographically defined battlefields must now operate within an environment characterised by anonymity, interconnected networks, and rapidly evolving technologies. The continued relevance of International Humanitarian Law depends not upon abandoning its foundational principles but upon adapting their implementation to contemporary realities.

[60] Roff & Moyes, *supra* note 44, at 4-9.
[61] U.N. Secretary-General, *supra* note 54.

 [ISSN 2581-5369]

The future regulation of military cyber operations should therefore be guided by three interconnected objectives: improving attribution, strengthening responsibility, and enhancing civilian protection. Together, these measures offer a more realistic path towards accountability than attempts to create entirely new legal regimes detached from existing international law. In this respect, the challenge confronting the international community is not whether cyber operations can be regulated, but whether legal institutions can evolve quickly enough to ensure that technological innovation does not outpace legal responsibility.

VII. CONCLUSION

Military cyber operations have fundamentally altered the character of contemporary conflict by enabling states to pursue strategic and military objectives through digital means that frequently operate beyond traditional battlefield boundaries. This study has demonstrated that although International Humanitarian Law remains applicable to cyber warfare through the principles of *jus ad bellum*, *jus in bello*, distinction, proportionality, and military necessity, its effective implementation is hindered by persistent challenges relating to attribution, state responsibility, and enforcement. The anonymity of cyberspace, the growing use of proxy actors, and the interconnected nature of civilian and military digital infrastructure have collectively created a significant accountability deficit within the digital battlespace. While international initiatives such as the Tallinn Manual 2.0 and United Nations cyber governance processes have contributed to the clarification of legal norms, they have not fully resolved the practical difficulties associated with assigning responsibility for unlawful cyber conduct. The paper therefore argues that the future effectiveness of International Humanitarian Law will depend not upon the creation of entirely new legal regimes but upon strengthening attribution standards, reinforcing state responsibility, protecting civilian digital infrastructure, and promoting greater international cooperation. In an era where cyber capabilities increasingly shape national security and global stability, ensuring accountability in cyberspace is essential for preserving both the legitimacy of international law and the humanitarian values that underpin it.

*****

 [ISSN 2581-5369]