REVIEW OF CRIME, PEACE AND SOCIETY
ISSN (O): 3079-6105, ISSN (P): 3079-6091
Vol. 3, No. 2, 2026, 281-298

REGULATING CYBER ATTACKS IN ARMED CONFLICTS UNDER INTERNATIONAL HUMANITARIAN LAW: A LEGAL FRAME WORK

Muhammad Munir [1], Dr. Muhammad Idrees *[2]

Abstract

Protection of civilians and non-military infrastructure has always been a source of concern since inception of warfare. International humanitarian law provides protection to those not participating in the conflict. However, the paradigm shift of the warfare from purely kinetic to non-kinetic nature, where cyber has emerged as a fifth domain in the warfare has raised concerns over the inadequacy of international humanitarian law, primarily drafted for purely kinetic nature of warfare. This intricates cosmos of cyber warfare nurtures several queries regarding the inadequacies of international humanitarian law. The proposed research critically investigates existing international treaties, conventions and state practices regulating the cyber space to analyze relevance of these instruments in the battle fields powered by net-centric sensors and machine-controlled shooters grids. The research will address three core questions by employing doctrinal, qualitative and comparative analysis approaches. Firstly, the classification of cyber warfare under jus ad bellum and jus in bello, the classical principals of international law. Secondly, attribution of responsibility for the acts in cyber dominant environment characterized by obscurity and proxy activity. Thirdly, how the principles of proportionality, precaution and distinction can meaningfully be applied in cyberwarfare. The UN Charter (1945) and The Geneva Conventions (1949) along with the additional protocols (1977) forms the primary legal resources. Supplementary guidance is drawn from the Tallin Manual, contemporary state practices and International Committee of Red Cross (ICRC) work in addition to the analysis of recent incidents like Russia-Ukraine conflict to examine the doctrinal adequacy in real circumstances. The research is aimed to propose an all-inclusive legal framework to harmonize the conventional principles of international law with digital realities to safeguard effective protection of civilian on one hand while attributing accountability on the other hand, in the context of cyber warfare.

Article History
Received 29 March 2026
Revised 13 June 2026
Accepted 24 June 2026
Published 24 June 2026

Corresponding Author: *

Keywords
Cyber warfare: International Humanitarian Law: Armed conflicts: Protection of civilians: Legal frame work: Attribution

Introduction

Technological advancements in the new era have also changed the dynamics of warfare from kinetic to non-kinetic. The fifth dimension of warfare i.e. cyberwarfare has posed a new challenge both in military strategy as well as legal frame work, because the said domain of warfare is exploited both by the state and non-actors to target critical civilian infrastructure like power grids, medical and communication facilities severely effecting the civilians, yet the law is inadequate to address

[1], PhD Law Scholar, Hajveri Law College, TIMES University Multan goodmail109@gmail.com.
[2] Associate professor, TIMES University Multan. idreesabbas3@gmail.com

accountability (Gill T. D and Geiß, R 2020).

Cyber warfare has rapidly transformed beyond simple hacking to a full-scale capability of Armed conflict incorporating diverse cyber capabilities with conventional military tactics and operations, in the form of a new warfare termed as hybrid warfare characterized as technology-driven, aiming to collapse the enemy from within rather than destroy it physically (Mercado, V. A. 2025). Cyber has shown rampant progress in recent years becoming the important tool of warfare managing economic, societal and political domains as well as military operations. Although, on one hand it is contributing to the speedy growth, yet, it has simultaneously given exponential upsurge to the new means and methods of warfare, consequently, putting the security of all states at risk, by raising internal and external threats(Roscini, 2010). Such threats escalate to the cyberwarfare resulting to armed conflicts between States. The objectives of cyberwarfare are exactly the same as those attributed to kinetic use of force, i.e. including but not limited to waning the military potential of the adversary and to shift it in own advantage. Cyberwarfare like the kinetic warfare is also governed under the famous principles of International Law i.e. 'jus ad bellum' and 'jus in bello', where the former legalizes the 'use of force', whereas, the later regulates the conduct of war under International Humanitarian Law (IHL) and comes into motion, once an armed conflict has begun. It is aimed to reduce the humanitarian cost of said armed conflicts, thereby protecting those objects and persons, that offer no military advantage to any of the parties to the conflict (S. Haroon, 2017).

The first recorded use of cyber technology as a tool of warfare between the states is referred to the famous Estonian attacks in 2007, where the riots powered through social media, triggered by ethnic Russians were led in the streets of Estonia. Allegedly, the agitation was provoked by Russian government (National & 2011, n.d.). This organized social media movement transformed to the organized cyber-attacks, paralyzing Estonia's private and public systems for around ten days, besides denial of ambulance services for over an hour (LJ & 2011, n.d.).The attacker could not be recognized being the anonymous nature of the attacks as well as attacker. Despite the fact that Estonia was in a position to claim collective defense, being a member of NATO, however, the remedy could not be availed due to the unsigned nature of cyberwarfare.

Although, this incident does not fall under the ambit of IHL as the incident could not qualify to be an armed attack, hence IHL was not applicable. The incident could not capture the world's attention in the context of threat posed by cyber technology, however, very soon around 120-140 states engaged to develop the cyber warfare capability realizing the sensitivity of emerging tool of future warfare. In 2008, during the Russian invasion of Georgia the world realized cyber warfare as a really inevitable and factual threat during the future conflicts (Herzog, S. 2017).

Legal foundations of the armed conflicts like "prohibiting threat or use of force against any sovereign state" and "the right to self-defense against the belligerent state" are derived principally from the UN Charter (1945). Geneva Convention (1949) along with its additional protocols supplements the said legal frame work by providing the rules regarding conduct of hostilities, protection of civilians and hors de combats (Dormann, K. 2004). However, both the instruments do not provide sufficient frame work for regulation of cyber operation that disrupt as lethally as the conventional weapons (Murphy, S. D. 2021).

2. Research Problem

Although there is a growing consensus that means of warfare under the cyber space have no less significance than the conventional weapon systems. Likewise, IHL is equally applicable to the cyber

as it for the conventional domain, however, the inadequacies in the existing legal frame work raise certain queries regarding attribution and responsibility, threshold determination, applicability of IHL principles and the challenge of enforcement. The study will highlight the weaknesses and shortfalls of the existing International Humanitarian Law to afford protection of civilian population and infrastructure, not active part of hostilities. It is also aimed to regulate the conflict lying in the cyber space and to suggest, how it can be refined to afford protection and accountability.

2.1. Research Questions

a. Under what conditions and circumstances, cyber operations amount to 'use of force' or 'armed attack' under Article 2(4) and Article 51 of the UN Charter?

b. How the principles of distinction, proportionality and precaution as laid down by IHL would be interpreted to regulate cyber operations affecting essential civilian digital platforms?

c. How the evidentiary or procedural standards can enhance attribution and accountability for state and non-state actors in cyber operations?

2.2. Literature Review

Contemporary Developments and Legal Discourse – 2023 to 2025

Recent Russia–Ukraine conflict inspired a surge in contemporary analyses of the cyber dominated spectrum. Scholarly analysis of the conflict establishes that non-kinetic operations lying in the cyber domain in the form of disruption of power grids, denial of essential services and repudiation of data networks has the capability to inflict similar harm as that of physical destruction, therefore, the same type of operations should be treated as 'attacks' under international humanitarian law (Khalil, A. 2024). Biggio (2025) proposed a "loss of functionality" test that balances military necessity with humanity, suggesting that the focus should shift from physicality to affect (Biggio, G. 2025). It has been resonated by the ICRC's 2024 statement in the UN Security Council, emphasizing to recognize that civilian population may suffer from digital disruption even without physical harm (ICRC, 2024). Concurrently, the Center for Strategic and International Studies (CSIS) recognized numerous state-sponsored cyber incidents, escalating the risks to civilian infrastructure. Such a comprehensive analysis leads to an inference that the existing legal instruments are inadequate to ensure deterrence and effectively punish the violators. Although Tallinn Manuals are the key reference for the cyber operations, yet they are devoid of any binding force. Also, these manuals failed to fetch an undisputed opinion from all states, including those propagating cyber sovereignty (Boylan, E. 2017).

The cyber space as a domain which is dynamic as well as unsettled and is characterized by increasing consensus on the significance of international humanitarian law, however, there is still a persistent divergence, how states and scholars interpret the basic principles of its thresholds, attribution and state responsibility (Pandey, A. 2025).

Doctrinal Refinement and State Practices - 2020-2023

The key events shaping the legal framework includes the Estonian cyber-attack, 2010, Ukrainian power grid attacks, 2015 and the continued digital operations since 2022, during the recent Russia-Ukraine war (Mraz, P. 2025). Lieber and other scholars evaluated these important historic events with a view to have a check how the states have avoided or utilized the international legal arguments in the wake of these happenings and the outcome of the analysis was the divergent interpretation of the term 'use of force'. The researchers also began to integrate the concept of attribution of responsibility in the cases where evidence was either uncertain or vague (Dinstein, Y. 2022). The multifaceted nature of cyberspace is characterized by presence of proxies, hired hackers and unsigned infrastructure operators, undermining the conventional doctrine of state responsibility and attribution (Crawford, J. 2012).

Institutional Guidance/ Scholarly Work - 2013 to 2020

Tallin Manual 1.0 and Tallin Manual 2.0, both developed by the NATO Cyber Defense Centre of Excellence is the only authentic institutional guidance available related to the International Law applicable to the Cyber Warfare. These manuals, although non-binding, yet offer exceptional guidance regarding application of existing international laws to the cyber domain (Tikk & Vihul, L. 2010). These manuals established that during the armed conflict, cyber operations are likewise governed by the international humanitarian law as are the conventional kinetic operations, despite the fact that these have not yet been codified by the sates or ratified through treaties (Schmitt, 2013). Concurrently, International Committee of Red Cross (ICRC), has published several position papers, proclaiming that the Geneva convention (1949) along with its additional protocols (1979) are fully applicable to the cyber operations during armed conflict (Dormann, K. 2004). ICRC has established that the civilian population and the civilian infrastructure enjoy the similar protection by Geneva Convention against cyber operations as against conventional operations (Gisel. L, et al. 2020). ICRC has stressed that cyber operations against the non-military targets like power stations and hospitals may breach central principles of International Humanitarian Law.

Theoretical Foundations - Before 2015

During late 90's cyber emerged as a new domain of war, consequently a debate on this new form of warfare started which was principally focused on the aspect that, whether the cyber operations amounts to 'use of force' or 'armed attacks' under UN Charter (1945). Schmitt (2013) and Lin (2012) have identified the intangible nature of cyber warfare and highlighted the inadequacies of the traditional international legal frame work, primarily designed for kinetic operations, is unable to address the challenges of cyber operations (Droege, C. 2012). According to their opinion, international law specially Article 2 and 51 of the United Nations Charter was silent on the operations in virtual domain, particularly when the physical damage has not happened (Waxman, M. C. 2011). The scholarly debate identified two major questions with the divergent views, first, the non-kinetic nature of operations resulting to disruption or denial of services would be considered as "attacks" similar to those resulting for kinetic operations and second, how could the principles of distinction, necessity and proportionality, principally designed for kinetic operations, be applied to the operations in virtual domain (Berchev, D. 2025).

3. Research Methodology

The research uses Qualitative and doctrinal research design augmented by comparative analytical methods. The research analyses the existing legal norms and institutional guidelines for protection of civilians under IHL, in the wake of cyber operations. It focuses to determine the scope, applicability and limitations of IHL regarding cyber operations analyzing treaties, conventions, judicial decisions and scholarly writings. Comparative legal method juxtaposes IHL principles applicable to conventional conflicts with their extension to cyber operations, identifying consistencies, ambiguities and gaps in existing legal interpretations. The research also integrates an interpretivist stance, recognizing the dynamic nature of law that it is not static but shapes up through interpretation and scholarly engagement.

4. Strengths and Relevance of Existing Normative Architecture

The current norm-setting framework of cyber warfare is multi-layered and is composed of the UN Charter, IHL, customary international law and a growing collection of non-binding, interpretive documents (Schmitt, 2017; Tsagourias, 2023). These sources collectively offer the legal basis to evaluate the legality of cyber operations in peacetime and armed conflict. While these are all regimes which predate the advent of cyberspace as a space for military activity, they remain relevant to provide important normative guidance: the principle of technological neutrality, which states that the law applies to the conduct of armed forces regardless of the type of weapon or technology used (ICRC, 2024). Firstly, the existing structure is continuous. International law has been able to evolve over the course of successive technological revolutions without the need to replace the existing legal regimes (Dinstein, 2022). This evolutionary nature of cyber operations bolsters the case for the regulation of cyber operations to be based on the interpretation and development of existing principles rather than the formation of a new treaty. As the International Court of Justice stated in its Advisory Opinion on the "Legality of the Threat or Use of nuclear weapons" (1996), humanitarian principles should apply to all methods and means of warfare, regardless of technological developments. This has since been reiterated by the ICRC and is echoed in the reasoning of the experts of the Tallinn Manual (ICRC, 2024; Schmitt, 2017).

Secondly, the UN Charter remains the primary legal source of the international law of inter-state use of force. UN Charter, 1945, Articles 2(4) and 51 set out the bounds of normativity that cyber operations should be evaluated against. While opinions differ over the threshold of cyber activity that constitutes prohibited force or an armed attack, the Charter nevertheless offers an invaluable framework within which to examine issues of sovereignty, non-intervention, self-defence and collective security (Tsagourias, 2023; Henderson, 2024).

Thirdly, humanitarian principles of distinction, proportionality, precaution, military necessity and humanity are still conceptually able to control cyber operations. These principles are sufficiently flexible to allow for changing technologies as they are stated in functional, not weapons-specific terms. They have a general purpose of protecting civilians from unnecessary suffering and limiting the unnecessary suffering of civilians, regardless of how hostilities are fought (Dinstein 2022; ICRC 2024). Thus, even in a strongly digitalised conflict the existing framework still has a significant normative relevance.

4.1. Structural Weaknesses of the Existing Legal Framework

Although the principles underlying international law remain applicable, the current international legal framework has a number of structural flaws which seriously limit its effectiveness in controlling cyber warfare. These gaps are not just technical, but conceptual as well, demonstrating the lack of a conceptual anchoring of legal principles designed for kinetic warfare with the reality of cyberspace (Tsagourias, 2023). The main limitation with respect to cyber operations concerns the lack of internationally agreed definitions. There is currently no legal definition in international law of what constitutes a "cyber-attack", "cyber operation", "critical digital infrastructure" or "civilian data". This definitional imprecision gives rise to different understandings by the states and the international organisations, which results in a lack of legal clarity (Schmitt, 2017; Efrony & Shany, 2018). The Tallinn Manual 2.0 provides important interpretative guidance, but does not have binding legal force and is not always accepted by the states (Schmitt, 2017). This means that States still take diverse national stances on the legal definition of cyber activities, leading to fragmentation, not harmonisation, (United Nations, 2021).

Another structural weakness is the ongoing dependence on the physical consequence as the only basis for legal regulation. The common rules of armed attack and humanitarian protection and their further development into traditional doctrines of use of force, developed in an environment where warfare typically caused physical damage and deaths and this had a tangible impact (Dinstein, 2022). Today's cyber operations, however, often inflict far more serious social effects from functional disruption as opposed to physical harm. ICRC (2024); Tsagourias (2023): Disabling hospital networks, electricity power lines, banking systems, transport systems or emergency communications could affect civilian lives, but not necessarily tangible objects. While some of these types of harm have been recognized by existing law, they often have not received sufficient development of methodologies to be assessed meaningfully and consistently, which leads to different interpretations of the law and uncertainty about what actions a state can take (Schmitt & Vihul, 2023).

A further disadvantage is the fragmentation in international cyber governance. Currently, there is a fragmented legal framework that encompasses the UN, international and regional legal frameworks, domestic legal systems, voluntary confidence-building measures and technical standards by non-state actors (United Nations, 2021). Each is involved in the governance of cyberspace but often has overlapping authority that does not result in a coherent regulatory approach. This institutional fragmentation makes coordination more difficult, hinders the enforcement of the law and allows states to selectively enforce the law in their pursuit of strategic interests (Efrony & Shany, 2018). There is also a structural imbalance between technological innovation and legal development, which is identified in the research. The development of cyber capabilities is moving much faster than that of international law-making. Cyber treaty negotiation and customary law formation are relatively slow processes and require consensus across the States, while AI-powered cyber operations and autonomous cyber capabilities continue to drive the shift in the cyber threat landscape (Henderson, 2024; Tsagourias, 2023).

Lastly, there are no effective institutional arrangements for implementation and enforcement. In contrast to some other specialized areas of international law, there is no permanent international body to investigate cyber incidents, to establish attribution, to monitor compliance or to help in dispute resolution (United Nations, 2021; Schmitt & Vihul, 2023). The result is that implementation is dependent on largely unilateral state evaluations and political choices, which limits the objectivity and legitimacy of international legal reactions.

4.2. Regulating Cyber-Attacks: A Legal Framework

The foregoing discussion has shown that while international law already offers a general framework for the rules governing cyber operations in armed conflict, there are still many doctrinal gaps, institutional divisions and enforcement gaps that make it ineffective in real practice. These regulatory voids are now being capitalized on by modern cyber operations specially in terms of civilian protection, attribution, and state responsibility and accountability. Today, IHL's applicability to cyberspace is no longer the question but rather how the existing principles of IHL can be and should be, systematically interpreted and operationalised to effectively address the changing nature of digital warfare (International Committee of the Red Cross [ICRC], 2024; Tsagourias, 2023).

The future regulation of cyber warfare should not be based on the negotiation of an entirely new comprehensive treaty. The concept of a dedicated cyber warfare convention has been the subject of scholarly discussion but it is difficult to see how such a treaty can be put in place in the near future, given political disagreements among technologically advanced states, the lack of a common cyber warfare strategy and the swift speed at which technologies are developing (United Nations, 2021). Rather, the way forward is through the gradual evolution, interpretation and convergence of the present international legal regime, through state practice, judicial pronouncements, multilateral cooperation and authoritative guidance. For these reasons, this section suggests a coherent international legal system that would bolster the existing regulation of cyber-attacks in armed conflicts without the intent to replace or detract from it. The proposed framework aims at decreasing the legal uncertainty, strengthening humanitarian protection, strengthening accountability and increasing consistency in the interpretation and application of IHL and the United Nations Charter.

4.3. Foundational Principles of the Proposed Legal Framework

4.3.1 Technological Neutrality

The technological neutrality, means that all technologies are treated equally. IHL does not govern with respect to technology. Cyber is therefore not an exception to the rule of law because it is conducted through a digital not a kinetic channel (Schmitt, 2017; ICRC, 2024). Emerging technologies can be controlled with existing normative bases in the Geneva Conventions and Additional Protocol I so far as humanitarian goals are upheld.

4.3.2 Humanity

The final goal of humanitarian law is the protection of persons who are not or no longer, taking part in hostilities. It is not removed regardless of whether the operations are carried out using conventional, autonomous or malicious means. Therefore, there must be equal legal safeguards for civilian populations against cyber operations that could disrupt health services, electricity, financial services, water, communications and other vital public infrastructure (Dinstein, 2022; ICRC, 2024).

4.3.3 Legal Certainty

Legitimate regulation would require law-making that was predictable, allowing states to decide what is legal and what is not before deciding to take action. Unclear legal reference points allow for tactical use and different practices from state to state. The focus of the framework is thus on legal definition and harmonised standards of interpretation.

4.3.4 Accountability

Accountability is an indispensable component of cyber governance. Ability to investigate, attribute and remedy violations of international legal obligations to prevent, deter or take appropriate action is of extreme importance. The proposed framework therefore includes technical, legal and institutional accountability provisions.

4.3.4 International Cooperation

Last but not least, cyber threats are global in nature. There is no one state with enough technical and legal expertise to manage cyberspace alone. Building effective governance, however, is dependent on the cooperation of a number of parties, sharing of information, cooperation on legal assistance and the coordination of institutions, particularly by the United Nations and relevant regional organisations (United Nations, 2021).

4.4 Uniform Definition of Cyber-Attack

Lack of uniformity in the legal definition of a "cyber-attack" was one of the main gaps that were found across the entire study. The terminology used in the existing international instruments is different, such as "cyber operations," "ICT activities," "malicious cyber activities" and "computer network attacks" with no clear distinction of the legal consequences involved (Schmitt, 2017; Efrony & Shany, 2018). Such terminological confusion has led to different practices in the states and to a variety of interpretations. The proposed framework calls for the adoption of an internationally recognised legal definition which would differentiate cyber-attacks from other cyber activity based on the attack's purpose and not the technical nature of the attack.

4.5 Distinction between Use of Force and Armed Attack

The potential legal implications of the difference between prohibited use of force under Article 2(4) of the UN Charter and an armed attack which triggers an inherent right of self-defense

under Article 51 (United Nations, 1945) has been one of the most contested aspects of international cyber law. Current case law offers little guidance on cyber operations as the traditional distinction was fashioned mainly in connection with kinetic military operations. This study suggests an effect based multi-factors threshold test of the following criteria:

- consequences to level of scale;
- duration of disruption;
- reversibility of damage;
- direct impact on civilian populations;
- damage to critical infrastructure;
- the importance of the targeted system for military purposes;
- foreseeability of humanitarian consequences;
- The effects of combined cyber campaigns.

The model would have no single factor determining. Instead, decision makers would evaluate the overall impact of a cyber operation based on the cumulative impact of these factors. In doing so, it has taken into account the operational characteristics of cyberspace and aligned itself with the jurisprudence of the International Court of Justice regarding the "scale and effects" doctrine. Implementing an internationally recognised threshold test would significantly decrease the uncertainty around state actions and would dissuade strategic use of legal ambiguities.

5. Proposed International Legal Framework for Regulating Cyber-Attacks During Armed Conflict

5.1 Rationale for a Coherent International Legal Framework

The above analysis shows that the current body of international law comprising the UN Charter, IHL, the law of state responsibility and customary international law offers a legal framework to govern cyber operations but is fragmented and grossly out-of-date in terms of its application to the operational realities of cyberspace. The current legal framework is weakened by ambiguities regarding ‘attribution', ‘thresholds of force', civilian protection and accountability (ICRC, 2024; Schmitt, 2017). The purpose of a coherent international legal framework is not to supplant IHL, but rather to make clear, harmonise and enhance the application of IHL to cyber warfare, while maintaining the humanitarian principles of IHL.

The principles of humanity, military necessity, distinction, proportionality, precaution, accountability and technological neutrality form the basis of the proposed framework. It aims to establish a set of legal principles that is predictable; is applicable to all civilians; is applicable to the behaviour of States; and is conducive to international collaboration in cyber operations.

5.2 Internationally Accepted Definition of Cyber-Attack

One of the main shortcomings of the existing legal framework is the lack of a common legal definition of cyber-attack. The terminology used in existing instruments is inconsistent, including "cyber operation," "malicious ICT activity" and "computer network attack," which leads to uncertainty in the practice of states and in interpretation by the law (Schmitt, 2017). Based on the above, the following definition is proposed:

A cyber-attack is a deliberate cyber operation that is part of an armed conflict and is intended or reasonably expected to cause damage, disable, destruction or significant impairment to a digital system, data, or networked infrastructure that has or is likely to have significant military, humanitarian, economic or societal consequences.

This definition acknowledges that cyber-attacks can have legally relevant impacts even if there is no material damage, so it is in keeping with current cyber warfare. There are a number of benefits to this definition. First, it is technologically neutral and thus can accommodate future technological developments. Secondly, it acknowledges that cyber operations can have legally relevant consequences without causing damage. Thirdly, it integrates functional impairment and data manipulation into the concept of attack, capturing the essence of modern-day warfare. An adoption of such a definition would minimize the inconsistencies in state practice and also give a shared legal terminology for national governments, courts and international organisations.

5.3 Clarifying the Threshold of Use of Force and Armed Attack

The Threshold of Use of Force and Armed Attack is clarified. Whether a cyber operation is a prohibited use of force under Article 2(4) of the UN Charter or an armed attack under Article 51 is one of the most controversial aspects of cyber law. Current state practice is not homogeneous and there is no consensus on what threshold is considered acceptable (Tsagourias, 2023). This study suggests an effect based, multi-factors assessment that includes:

• the consequences of things are large and serious;
• duration of disruption;
• physical and psychological consequences;
• effect on critical civilian infrastructure;
• reversibility of harm;
• the threat to the target;
• coordinated cyber operations' cumulative consequences;
• anticipation of civilian casualties.

This flexible assessment will remove rigidity, achieve legal certainty and consistent application of the assessment.

5.4 Enhanced Protection of Civilian Digital Infrastructure and Data

It is now essential to have critical information infrastructure in order to enjoy fundamental human rights and to survive civilian populations in the digital transformation of modern

societies. Hospitals, electric power grid, water treatment plants, banking systems, emergency communications, transportation systems and satellite services are now considered critical civilian infrastructure. While current IHL has protections for civilian objects, there are unclear implications of the legal status of civilian data and digital infrastructure. For this reason, it is suggested that the following measures be taken as part of the proposed framework:

- Essential civil infrastructure digital elements should be explicitly identified as ECOs; Civilian data, such as medical, humanitarian and emergency-response data, should be protected in the same way as physical civilian objects;
- Cyber operations intended to disrupt critical public infrastructure must be considered illegal, unless they are legally justified by the necessity of the military and proportional;
- A dual-use infrastructure should be evaluated with a contextual balancing test with significant consideration to the potential for civilian harm.

5.5 International Standards for Attribution

The key challenge to successful cyber warfare regulation is attribution. Technical anonymity allows states and non-state actors to cover their tracks with proxy networks, intermediary infrastructureand advanced deceptive tactics. The proposed framework calls for internationally agreed upon standards of attribution to be based on:

• technical forensic evidence;
• intelligence assessments subject to appropriate safeguards;
• digital chain-of-custody requirements;
• independent expert verification;
• collating the circumstantial evidence;
• transparent evidentiary procedures.

It should not be reliant on any single evidence source, but rather cumulative assessment that can meet international standards of proof.

5.6 Strengthening State Responsibility

While the Articles on Responsibility of States for Internationally Wrongful Acts offer useful legal guidance, there is a need for more clarity in the context of cyber operations on the due diligence requirements. States should thus be obliged to:

- Stop them from knowingly using their territory for internationally wrongful cyber operations; • examine important malicious cyber activity which emanates from their territory;
- Cooperate in international investigations;
- Maintain pertinent digital evidence;
- Make adequate reparation for conduct which is internationally wrongful.

When these obligations are not complied with, this should be considered a violation of international law, even in the absence of an active role in the cyber operation.

5.7 Establishment of an International Cyber Investigation Commission

One of the major problems of the current legal system is the lack of a neutral institutional means to investigate cyber incidents. The concept of an International Cyber Investigation Commission (ICIC) under the umbrella of the UN is recommended in this article. It would have the main purpose of:

• technical investigation of critical cyber incidents;
• assistance in attribution;
• the preservation of electronic evidence;
• independent publishing;
• cooperation between states in their own interests for the benefit of others;
• developing technical standards;
• support in international dispute resolution.

The Commission would not have judicial powers but its conclusions would offer an objective ground for international legal action.

5.8 Accountability and Enforcement

The suggested framework besides ensuring credible systems of accountability essential to effective regulation calls for:

- Established a legal framework for combating cyber-crime crimes and offences; improved communication among investigators and criminal justice authorities on an international level;
- Restrictions on imports and exports, as well as on travel across borders;
- Strengthened measures for restoration of affected states;

International audit of compliance; and Reporting to the UN on a periodic basis.
These would make compliance to existing international legal obligations more compelling and enhance deterrence.

5.9 Role of the United Nations

UN should take a more proactive and active approach to cyber governance as follows:

- Creation of interpretative guidance on IHL and cyberspace;
- Establishment of a mutual understanding of how to approach the situation;
- Assistance with capacity building for developing States;
- Developing a code of conduct for accountants;

- More robust Open-Ended Working Group process;
- Encouragement of progressive development of customary international law.

The first step should be the U.N. clarifying through interpretation and coordinating institutions, rather than renegotiating a new treaty.

5.10 Benefits of the Proposed Framework

- Reduce legal uncertainty;
- Strengthen civilian protection;
- Develop uniformity of state practice;
- Facilitate attribution;
- Enhance accountability;
- Encourage peaceful resolution of conflicts;
- Reinforce compliance with International Humanitarian Law;
- Preserve international peace and security in cyberspace.

The framework has the advantage of combining old and new legal concepts with the new technological realities, thereby offering a practical approach to reinforce international regulation while maintaining the stability of the existing legal order.

6. Recommendations

The findings of this study support the following recommendations:

1. States should adopt internationally harmonised definitions of cyber-attacks and cyber operations to reduce interpretative inconsistency.

2. The UN should develop authoritative interpretative guidance clarifying the application of Articles 2(4) and 51 of the UN Charter to cyber operations.

3. The ICRC should continue elaborating the application of distinction, proportionality, precaution and military necessity to cyber warfare, particularly regarding civilian digital infrastructure and data.

4. States should recognise essential civilian digital infrastructure including healthcare systems, electricity networks, financial systems, telecommunications and emergency services as specially protected civilian objects during armed conflict.

5. International legal standards for cyber attribution should be developed through multilateral negotiations, combining technical forensic evidence with transparent legal procedures.

6. States should strengthen domestic legislation implementing International Humanitarian Law obligations applicable to cyber operations and improve national cyber resilience.

7. An independent International Cyber Investigation Commission should be established under the auspices of the UN to facilitate impartial investigations and technical attribution.

8. States should strengthen due diligence obligations by preventing malicious cyber activities originating from their territory and by cooperating fully in international investigations.

9. International organisations should expand technical assistance and capacity-building programmes to enable developing countries to implement cyber governance obligations effectively.

10. Future developments of international law should focus on interpretative clarification and progressive codification rather than the immediate negotiation of a comprehensive new cyber warfare treaty.

7. Conclusion

Cyber warfare represents one of the most significant legal challenges confronting contemporary international law. As societies become increasingly dependent upon interconnected digital infrastructure, the humanitarian consequences of cyber operations are likely to become more severe, more transnational and more difficult to regulate. This article has demonstrated that International Humanitarian Law remains applicable to cyber operations conducted during armed conflict through the principle of technological neutrality. Nevertheless, the practical application of existing legal rules continues to be hindered by uncertainty concerning the legal thresholds of use of force and armed attack, the protection of civilian digital infrastructure and data, attribution, state responsibility and accountability.

The analysis further establishes that these deficiencies do not arise from the absence of international law but from fragmentation, inconsistent interpretation and limited institutional implementation. Existing legal principles continue to provide an essential normative foundation; however, they require progressive clarification to respond effectively to contemporary technological realities.

The principal contribution of this article lies in proposing a coherent international legal framework that integrates existing principles of International Humanitarian Law, the United Nations Charter and the law of state responsibility into a structured and operationally effective regulatory model. By introducing harmonised legal definitions, clearer attribution standards, enhanced protection for civilian digital infrastructure, strengthened due diligence obligationsand an independent international investigative mechanism, the proposed framework addresses many of the doctrinal and practical deficiencies identified throughout the study.

Ultimately, the future regulation of cyber warfare should be guided not by the creation of entirely new legal regimes but by the progressive interpretation, harmonisationand institutional strengthening of existing international law. Such an approach preserves legal continuity while ensuring that humanitarian principles remain capable of protecting civilian populations in an increasingly digital battlespace. Continued cooperation among states, international organisations, legal scholarsand technical experts will be indispensable for maintaining the relevance, legitimacyand effectiveness of International Humanitarian Law in the face of rapidly evolving cyber threats.

References

Berchev, D. (2025, January). The principle of proportionality in international humanitarian law: legal foundations and contemporary challenges. In Proceedings of the Annual University Scientific Conference (Print), Vol. 8, pp. 217-228. Veliko Tarnovo:"V. Levski" National Military University Publishing Complex, June 05-06, 2025. ISSN 1314-1937.

Biggio, G. (2025). Regulating non-kinetic effects of cyber operations: the 'Loss of Functionality' approach and the military necessity-humanity balance under International Humanitarian Law. *Journal of Conflict and Security Law.*

Bisson, D. M. (2014). Cyber Power Restrained: How Strategic Culture Inhibits the Integration of Cyber Weapons by the United States Military.

Boylan, E. (2017). Applying the Law of Proportionality to Cyber Conflict: Suggestions for Practitioners. Vand. J. Transnat'l L., 50, 217.

Crawford, J. (2012). Articles on responsibility of states for internationally wrongful acts. *United Nations Audiovisual Library of International Law*, 3.

Dinstein, Y. (2022). *The conduct of hostilities under the law of international armed conflict* (4th ed.). Cambridge University Press.

Dinstein, Y. (2019). *The international law of belligerent occupation* (2nd ed.). Cambridge University Press.

Dormann, K. (2004, November). Applicability of the Additional Protocols to computer network attacks. In *International Expert Conference on Computer Network Attacks and the Applicability of IHL, Stockholm* (p. 3).

Doswald-Beck, L. (1997). International humanitarian law and the Advisory Opinion of the International Court of Justice on the legality of the threat or use of nuclear weapons. *International Review of the Red Cross (1961-1997)*, *37*(316), 35-55.

Droege, C. (2012). *Get off my cloud: Cyber warfare, international humanitarian lawand the*

protection of civilians. *International Review of the Red Cross*, 94(886), 533–578.

Duncan B. Hollis, 'An e-SOS for Cyberspace' [2011] 52(2) Harvard International Law Journal 375

Efrony, D., & Shany, Y. (2018). A rule book on the shelf? Tallinn Manual 2.0 and subsequent state practice. American Journal of International Law, 112(4), 583–657.

Gill, T. D., Geiß, R., & Krieger, H. (Eds.). (2020). *Yearbook of international humanitarian law: Vol. 23 (Cyber warfare and international law)*. T.M.C. Asser Press.

Gisel, L., Rodenhäuser, T., & Dörmann, K. (2020). Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International Review of the Red Cross*, *102*(913), 287-334.

Green, L. C. (2018). *The contemporary law of armed conflict* (3rd ed.). Manchester University Press.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). *The law of cyber-attack. California Law Review,* 100(4), 817–885.

Haroon, S. (2017). International Humanitarian Law on Cyberwarfare and Pakistan's Legal Framework. *Available at SSRN 3051009*.

Henckaerts, J. M., & Doswald-Beck, L. (Eds.). (2005). *Customary international humanitarian law: Vol. I (Rules)*. Cambridge University Press.

Henderson, I. (2024). The contemporary law of targeting (2nd ed.). Brill.

Herzog, S. (2017). Ten years after the Estonian cyberattacks: Defense and adaptation in the age of digital insecurity. *Geo. J. Int'l Aff.*, *18*, 67.

Hollis, D. B. (2011). An e-SOS for Cyberspace. *Harv. International Law Journal*, *52*, 373.

International Committee of the Red Cross. (2024). International humanitarian law and the challenges of contemporary armed conflicts. ICRC.

International Committee of the Red Cross (ICRC). (2021). *International humanitarian law and cyber operations during armed conflicts*. ICRC Position Paper.

Kellenberger, J. (2011). International humanitarian law and new weapon technologies. *34th round table on current issues of international humanitarian law. San Remo,* 8-10.

Khalil, A., Bitar, M., & Raj, S. A. K. (2024). Navigating legal frontiers in cyber warfare: Insights from the Russia-Ukraine conflict. *The Lawyer Quarterly*, *14*(2).

Lin, H. (2012). Cyber conflict and international humanitarian law. International review of the Red Cross, 94(886), 515-531.

Lubell, N. (2020). *Extraterritorial use of force against non-state actors under international law*. Oxford University Press.

Melzer, N. (2011). *Cyber warfare and international law*. UNIDIR Resources. United Nations Institute for Disarmament Research.

Mercado, V. A. (2025). Cyber Warfare and the Future of Conflict.

MRÁZ, P. (2025) towards A regular institutional dialogue on international information and communication technology security.

Murphy, S. D. (2021). *Principles of international law* (3rd ed.). West Academic Publishing.

Pandey, A. (2025). Application of International Humanitarian Law in Changing Dimensions of Armed Conflict vis-à-vis Cyber Warfare. *Unity Journal*, *6*(1), 284-296.

Roscini, M. (2010). Worldwide warfare: Jus ad bellum and the use of cyber force. Martinus Nijhoff.

Shaw, M. N. (2021). *International law* (9th ed.). Cambridge University Press.

Solis, G. D. (2021). *The law of armed conflict: International humanitarian law in war* (3rd ed.). Cambridge University Press.

Sassòli, M. (2024). *International humanitarian law: Rules, controversies and solutions to problems arising in warfare*. Edward Elgar Publishing.

Schmitt, M. N., & Vihul, L. (2019). *The nature of international law cyber norms*. In H. Krieger, T. D. Gill, & R. Geib (Eds.), *Yearbook of international humanitarian law: Vol. 22* (pp. 3–32). T.M.C. Asser Press.

Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.

Schmitt, M. N., & Vihul, L. (2023). The nature and future of international law in cyberspace. Texas Law Review, 101(3), 619–670.

Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

Schmitt, M. N. (Ed.). (2013). *Tallinn Manual on the international law applicable to cyber warfare*. Cambridge University Press.

Tsagourias, N. (2023). Cyber warfare and international law (2nd ed.). Oxford University Press.

Tikk, E., Kaska, K., & Vihul, L. (2010). *International cyber incidents: Legal considerations*. Cooperative Cyber Defence Centre of Excellence.

United Nations. (1949). *Geneva Conventions (I–IV)*. United Nations Treaty Series.

United Nations. (1977). *Protocol Additional to the Geneva Conventions of 12 August 1949 relating to the Protection of Victims of International Armed Conflicts (Protocol I)*. United Nations Treaty Series.

United Nations. (1977). *Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II)*. United Nations Treaty Series.

United Nations. (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174)*.

United Nations. (1945). Charter of the United Nations. https://www.un.org/en/about-us/un-charter

United Nations. (2021). Report of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security (A/75/816). United Nations.

Walker, P. A. (2011). Rethinking Computer Network" Attack": Implications for Law and US Doctrine. *American University National Security Law Brief*, *1*(1), 3.

Waxman, M. C. (2011). *Cyber-attacks and the use of force: Back to the future of Article 2(4)*. *Yale Journal of International Law*, 36(2), 421–459.