International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cyber Warfare and International Humanitarian Law: Are Existing Laws Sufficient?

Md. Nahid Hasan Chowdhury Rifat[1], Kh. Sabbir Hasan[2], Sharina Islam Fima[3]

[1,2,3]Student, Department of Law, Bangladesh University of Professionals

Abstract

The rapid growth of digital technology has changed cyberspace into a new battleground, raising serious legal and humanitarian issues for the international community. Cyber warfare has increasingly become a way to wage modern conflict. It can disrupt critical infrastructure, financial systems, healthcare services, military operations, and civilian communications without using traditional weapons. However, the changing nature of cyber-attacks brings up a key question: is existing International Humanitarian Law (IHL) adequate to regulate such actions during armed conflict?

This paper examines whether current IHL principles, especially distinction, proportionality, military necessity, and state responsibility, can effectively address the complexities of cyber warfare. The study looks at relevant international legal documents, such as the Geneva Conventions, Tallinn Manual 2.0, and customary international law, along with recent cyber incidents involving state and non-state actors. It argues that while existing IHL principles offer a basic framework for regulating cyber operations, there are still significant legal uncertainties about attribution, civilian protection, the threshold for armed attack, and accountability mechanisms.

The paper also explores the challenges that developing countries face when responding to cyber threats due to their technological and legal limitations. Finally, the study suggests creating clearer international norms and collaborative mechanisms to ensure effective humanitarian protection in cyberspace. The research aims to add to current discussions on updating international law to reflect the realities of digital conflict in the twenty-first century.

Introduction

"*Wars are no longer fought only with bullets and bombs; they are increasingly fought through keyboards and code.*" [1]

The fast growth of information and communication technology has changed warfare in the twenty-first century. Cyberspace has become a new area for operations, like land, sea, air, and outer space. This change allows both countries and non-state groups to carry out attacks using digital networks and computer systems.

Unlike conventional warfare, cyber warfare allows attackers to disrupt critical infrastructure, steal sensitive information, manipulate communication systems, and disable governmental or military operations without crossing physical borders. The increasing dependence of modern societies on digital

[1] David E Sanger, The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age (Crown Publishing 2018)

technologies has therefore made cyber operations one of the most significant security concerns of the contemporary international order.

The strategic importance of cyberspace in modern warfare has become increasingly visible through several major cyber incidents over the past two decades. One of the earliest and most significant examples was the Stuxnet attack discovered in 2010, a sophisticated malware operation reportedly targeting Iran's nuclear facilities. The attack demonstrated how cyber tools could cause physical destruction to critical infrastructure without traditional military force. [2] Similarly, the 2007 cyber attacks against Estonia disrupted banking, media, and governmental institutions, illustrating the vulnerability of highly digitized states to coordinated cyber operations. [3]

More recently, cyber warfare has played a crucial role in the ongoing Russo-Ukrainian War. Since the escalation of the conflict in 2022, cyber-attacks have targeted Ukrainian government systems, communication networks, financial institutions, and energy infrastructure. These attacks have often accompanied conventional military operations, demonstrating the growing integration of cyber capabilities into modern armed conflict. [4] The conflict has also highlighted the challenges of attribution, state responsibility, and civilian protection under international law.

Another alarming example is the WannaCry ransomware attack of 2017, which affected more than 150 countries and severely disrupted hospitals, businesses, transportation systems, and public services worldwide. The attack exposed the global vulnerability of interconnected digital systems and revealed how cyber operations could generate humanitarian and economic consequences far beyond national borders. [5] Such incidents demonstrate that cyber warfare is no longer a theoretical or future threat; rather, it has become a practical reality affecting international peace and security.

The growing prevalence of cyber warfare raises serious concerns regarding the adequacy of existing international legal frameworks, particularly International Humanitarian Law (IHL).

IHL, primarily embodied in the Geneva Conventions of 1949 and their Additional Protocols, was originally developed to regulate conventional armed conflicts and to protect civilians during warfare. However, the unique characteristics of cyber operations; including anonymity, speed, transnational reach, and difficulties in attribution; create substantial legal uncertainties. Questions remain regarding when a cyber operation constitutes an "armed attack," how principles such as distinction and proportionality apply in cyberspace, and how accountability can be ensured for unlawful cyber conduct.

The central research problem of this study is whether the current framework of International Humanitarian Law is sufficient to regulate cyber warfare effectively in the digital age. Although existing legal principles provide a foundational framework, many scholars and policymakers argue that current laws remain inadequate to address the complexities of cyber operations conducted by both states and non-state actors.

Accordingly, the primary objective of this research is to assess the adequacy of existing legal frameworks governing cyber warfare under International Humanitarian Law. The study further seeks to analyze the applicability of IHL principles to cyber operations, identify major legal gaps and practical challenges, evaluate issues relating to civilian protection and state responsibility, and recommend possible reforms for strengthening international legal regulation in cyberspace.

[2] Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon (Crown 2014).
[3] https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf?utm
[4] https://www.icrc.org/en/document/short-papers-on-international-humanitarian-law-and-cyber-operations-during-armed-conflicts?utm
[5] https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst?utm

1. To achieve these objectives, the research addresses several key questions:
2. What constitutes cyber warfare and how does it differ from conventional warfare?
3. To what extent does International Humanitarian Law apply to cyber operations?
4. What are the major legal challenges associated with regulating cyber warfare?
5. Are current international legal frameworks sufficient to ensure civilian protection and state accountability?
6. What reforms are necessary to improve the regulation of cyber warfare under international law?

The scope of this study is limited to cyber warfare occurring within the context of armed conflict and the applicability of International Humanitarian Law to such operations. While the research discusses issues relating to cyber security and cyber-attacks generally, it does not extensively examine domestic cybercrime laws or purely economic cyber offenses unrelated to armed conflict.

This research adopts qualitative and doctrinal legal research methodology. The study primarily relies on secondary sources, including international treaties, customary international law, scholarly books, journal articles, reports of international organizations, and case studies relating to significant cyber incidents.

Emphasis is placed on legal instruments such as the Geneva Conventions, the United Nations Charter, and the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, alongside reports published by the International Committee of the Red Cross and the United Nations.

Ultimately, this study argues that while existing International Humanitarian Law principles remain applicable to cyber warfare, significant legal ambiguities and enforcement challenges continue to undermine effective humanitarian protection in cyberspace. As cyber operations increasingly shape modern conflicts, the international community must reconsider whether traditional legal frameworks can address the realities of digital warfare in the contemporary era.

Concept and Evolution of Cyber Warfare

A. Definition of Cyber Warfare

Meaning of Cyber Warfare

Cyber warfare refers to the use of digital technologies, computer networks, and cyber capabilities by states or organized groups to attack, disrupt, damage, or gain unauthorized access to another state's information systems, infrastructure, or military operations during conflict. It represents a modern form of warfare conducted through cyberspace rather than conventional physical battlefields.

The North Atlantic Treaty Organization defines cyber warfare as hostile actions conducted in cyberspace that can produce effects comparable to traditional military operations. Similarly, the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations explains that cyber operations may amount to armed attacks when they cause physical destruction, injury, or severe disruption to critical systems. [6]

Cyber warfare differs from conventional warfare because cyber-attacks can be launched remotely, anonymously, rapidly, and across international borders without direct military presence. Modern societies rely heavily on digital infrastructure, making cyberspace an attractive and effective domain for strategic attacks.

According to the International Committee of the Red Cross, cyber operations during armed conflict may affect hospitals, electricity networks, transportation systems, banking sectors, and communication infras-

[6] https://ccdcoe.org/research/tallinn-manual/?utm

tructures, thereby posing serious humanitarian risks. [7]

Characteristics of Cyber Warfare

Cyber warfare possesses several unique characteristics that distinguish it from traditional military conflict.

1. Anonymity and Attribution Difficulty

One of the most significant features of cyber warfare is the difficulty in identifying the actual perpetrator of a cyber-attack. Attackers often conceal their identities through proxy servers, encryption, and decentralized networks, making attribution legally and technically challenging.

2. Borderless Nature

Cyber operations can be conducted from any location in the world without physical intrusion into another state's territory. This transnational nature complicates jurisdictional and legal responses.

3. Speed and Low Cost

Cyber-attacks can occur within seconds and often require fewer financial resources compared to conventional military operations. A relatively small group of skilled individuals can inflict substantial damage on critical systems.

4. Civilian-Military Interconnection

Modern civilian infrastructure, including healthcare systems, financial institutions, and communication networks, is closely interconnected with military systems. Consequently, cyber-attacks may significantly affect civilians even when military objectives are targeted.

5. Asymmetrical Warfare

Cyber warfare enables weaker states and non-state actors to challenge technologically advanced states without maintaining large military forces.

Types of Cyber Attacks

Cyber warfare includes various forms of cyber-attacks depending on the objective and method employed.

A. Malware Attacks

Malware refers to malicious software designed to infiltrate, damage, or disable computer systems. Viruses, worms, spyware, and ransomware fall within this category.

Example: The WannaCry ransomware attack in 2017 disrupted hospitals, businesses, and public services across more than 150 countries. [8]

B. Distributed Denial-of-Service (DDoS) Attacks

DDoS attacks overwhelm computer servers or networks with excessive traffic, causing systems to crash or become inaccessible.

Example: The 2007 Estonia cyber-attacks involved large-scale DDoS operations targeting governmental and banking institutions. [9]

C. Cyber Espionage

Cyber espionage involves unauthorized access to confidential information for intelligence gathering purposes. States frequently use cyber espionage to obtain military, political, or economic information.

D. Infrastructure Attacks

These attacks target critical national infrastructure such as electricity grids, water systems, transportation

[7] https://www.icrc.org/en/document/short-papers-on-international-humanitarian-law-and-cyber-operations-during-armed-conflicts?utm
[8] https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst?utm
[9] https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf?utm

networks, and nuclear facilities.

Example: The Stuxnet malware targeted Iran's nuclear centrifuges and caused physical destruction through cyber means. [10]

E. Information Warfare and Disinformation

Cyber operations are increasingly used to manipulate public opinion through fake news, propaganda, and social media influence campaigns.

B. Evolution of Cyber Warfare

Early Cyber Espionage

The origins of cyber warfare can be traced to the Cold War era when states began using computer systems for intelligence gathering and military communication. Initially, cyber operations primarily involved espionage activities rather than destructive attacks.

During the 1980s and 1990s, advances in information technology and internet connectivity increased the strategic value of cyberspace. Governments and intelligence agencies began developing offensive cyber capabilities to infiltrate foreign networks and collect classified information.

One early example was the "Moonlight Maze" cyber espionage operation discovered in the late 1990s, which allegedly targeted United States government networks and defense systems. [11]

Modern State-Sponsored Cyber Attacks

The twenty-first century witnessed the transformation of cyber operations from espionage tools into strategic weapons capable of causing physical and economic damage.

The discovery of Stuxnet in 2010 marked a turning point in cyber warfare history. Widely regarded as the world's first digital weapon, the malware specifically targeted Iran's nuclear program and demonstrated how cyber tools could produce physical destruction comparable to conventional military attacks. [12]

Subsequently, states increasingly integrated cyber capabilities into military and national security strategies. Countries such as the United States, Russia, China, Iran, and North Korea have been accused of conducting or supporting cyber operations against foreign governments and infrastructure.

The ongoing Russo-Ukrainian War further demonstrates the integration of cyber operations into conventional warfare. Cyber-attacks against Ukrainian communication systems, financial institutions, and energy infrastructure have accompanied military operations on the battlefield.[13]

Rise of Artificial Intelligence and Digital Warfare

Recent technological developments have introduced artificial intelligence (AI), machine learning, and autonomous systems into cyber warfare.

- AI enhances cyber capabilities by:
- Automating cyber-attacks,
- Identifying system vulnerabilities,
- Conducting rapid data analysis,
- Improving surveillance and intelligence gathering.

Autonomous cyber systems can now independently detect vulnerabilities and launch adaptive attacks wit-

[10] Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon (Crown 2014).
[11] https://oig.justice.gov/sites/default/files/archive/special/9704a/07cyber.htm?utm
[12] Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon (Crown 2014)
[13] https://blogs.icrc.org/law-and-policy/2023/03/07/towards-common-understandings-the-application-of-established-ihl-principles-to-cyber-operations/?utm

hout continuous human control. This development raises significant legal and ethical concerns regarding accountability, civilian protection, and compliance with International Humanitarian Law.

Moreover, AI-powered disinformation campaigns using deep fakes and automated social media manipulation increasingly threaten democratic institutions and international security.

The growing integration of AI into military cyber operations indicates that future warfare will likely become increasingly digital, automated, and technologically sophisticated.

C. Difference Between Cyber Warfare and Cybercrime

Although cyber warfare and cybercrime both involve unlawful activities conducted through cyberspace, they differ significantly in terms of objectives, actors, targets, and legal implications.

Basis of Comparison	Cyber Warfare	Cybercrime
Primary Objective	Political, military, or strategic goals	Financial gain or personal benefit
Main Actors	States or state-sponsored groups	Individuals or criminal organizations
Targets	Critical infrastructure, military systems, governmental institutions	Individuals, businesses, financial accounts
Legal Framework	International law and IHL	Domestic criminal law
Scale of Impact	National or international security threats	Economic or personal harm
Example	Stuxnet attack on Iran	Online banking fraud

Cyber warfare generally occurs within the context of armed conflict or hostile international relations, whereas cybercrime primarily concerns criminal activities motivated by economic interests.

However, the distinction is not always clear. Some cyber-attacks conducted by non-state actors may simultaneously involve criminal conduct and national security implications. Consequently, the evolving nature of cyberspace creates increasing overlaps between cybercrime, cyber terrorism, and cyber warfare.

International Humanitarian Law (IHL): Basic Principles

International Humanitarian Law (IHL), also known as the law of armed conflict, is a body of international law designed to regulate the conduct of warfare and minimize human suffering during armed conflict. The primary sources of IHL include the four Geneva Conventions of 1949, their Additional Protocols, customary international law, and various international treaties. Traditionally, these rules were developed to govern conventional military conflicts involving physical weapons and territorial battlefields. However, the emergence of cyber warfare has raised critical questions regarding the applicability of IHL principles to cyberspace.

The International Committee of the Red Cross has consistently maintained that cyber operations conducted during armed conflict are not beyond the reach of international law. According to the ICRC, existing principles of IHL apply to cyber warfare in the same manner that they apply to conventional military operations.[14] Nevertheless, applying these principles to cyber operations remains legally and practically challenging due to the unique nature of cyberspace.

[14] https://www.icrc.org/en/document/short-papers-on-international-humanitarian-law-and-cyber-operations-during-armed-conflicts?utm

This chapter examines the core principles of International Humanitarian Law and analyzes their relevance in regulating cyber warfare.

A. Principle of Distinction

The principle of distinction is one of the foundational rules of International Humanitarian Law. Under Article 48 of Additional Protocol I to the Geneva Conventions, parties to an armed conflict must always distinguish between civilians and combatants, as well as between civilian objects and military objectives. [15] Attacks may only be directed against legitimate military targets.

In conventional warfare, distinguishing between military and civilian targets is relatively straightforward. Military bases, weapons facilities, and armed forces generally constitute lawful military objectives. However, cyber warfare significantly complicates this distinction because civilian and military systems are often interconnected through shared digital infrastructure.

For example, civilian communication networks, internet service providers, banking systems, and satellite infrastructures may simultaneously support both civilian and military activities. Consequently, a cyber-attack targeting military communications could unintentionally disrupt hospitals, emergency services, or transportation systems used by civilians.

A particularly important question arises regarding whether a hospital's computer system can be considered a lawful cyber target. Under IHL, hospitals and medical facilities enjoy special protection and must not be attacked unless they are being used for military purposes outside their humanitarian functions. [16] Therefore, a cyber operation disabling a hospital's digital infrastructure will generally violate the principle of distinction if it affects civilian healthcare services.

The cyber-attacks against Ukrainian healthcare and energy systems during the Russo-Ukrainian War demonstrate how civilian infrastructure may become vulnerable during cyber conflict. Such attacks raise serious humanitarian concerns because disruptions to healthcare systems can endanger civilian lives without direct physical violence.

The principle of distinction therefore requires states conducting cyber operations to carefully identify military objectives and avoid targeting civilian digital infrastructure. However, the dual-use nature of cyberspace continues to create substantial ambiguity in practical applications.

B. Principle of Proportionality

The principle of proportionality prohibits attacks that may cause incidental civilian harm excessively in relation to the anticipated military advantage. Article 51(5)(b) of Additional Protocol I specifically prohibits attacks expected to cause disproportionate civilian damage. [17]

In cyber warfare, proportionality assessments are particularly difficult because the indirect consequences of cyber-attacks are often unpredictable. Unlike conventional weapons, cyber operations can spread rapidly across interconnected networks and affect systems beyond the intended target.

For instance, malware designed to disable a military communication network may unintentionally infect civilian hospitals, banking institutions, or transportation systems.

The 2017 WannaCry ransomware attack disrupted healthcare services worldwide, including hospitals within the United Kingdom's National Health Service, demonstrating how cyber-attacks can produce widespread humanitarian consequences. [18]

[15] https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-48?utm
[16] https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949/article-18?utm
[17] https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-51?utm
[18] https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst?utm

Similarly, cyber-attacks against electrical power grids may indirectly threaten civilian populations by disrupting water supply systems, emergency healthcare services, and food distribution networks. Even when the intended objective is military, the resulting civilian harm may become excessive and therefore unlawful under IHL.

The proportionality principle obliges states to evaluate foreseeable civilian consequences before launching cyber operations. However, the complexity of digital networks makes it difficult to accurately predict the full scope of damage that cyber-attacks may cause. This uncertainty represents one of the greatest legal and operational challenges in applying IHL to cyberspace.

C. Military Necessity

The principle of military necessity permits only those measures necessary to achieve a legitimate military objective and that are not otherwise prohibited under international law. Military actions must contribute directly to weakening the enemy's military capacity.

In the context of cyber warfare, military necessity may justify cyber operations aimed at disabling enemy command systems, military radar, or communication networks during armed conflict. Cyber operations can sometimes achieve military objectives with less physical destruction than conventional attacks, potentially reducing civilian casualties.

For example, a cyber-attack temporarily disabling an enemy's military communication system may be considered militarily necessary if it prevents armed attacks or protects national security interests. However, military necessity does not justify unrestricted cyber operations against civilian infrastructure.

The Stuxnet operation against Iran's nuclear facilities illustrates this debate. Although the malware specifically targeted nuclear centrifuges associated with Iran's nuclear program, it also demonstrated the potential of cyber tools to cause physical destruction through digital means.[19] Critics argue that such operations create dangerous precedents for future cyber conflicts.

The principle of military necessity therefore requires balancing military advantage against humanitarian concerns. Cyber operations must remain limited to legitimate military objectives and avoid unnecessary suffering or destruction.

D. Principle of Humanity

The principle of humanity prohibits methods of warfare that cause unnecessary suffering or superfluous injury. This principle reflects the broader humanitarian purpose of IHL: protecting human dignity during armed conflict.

Cyber warfare presents unique humanitarian risks because attacks on digital infrastructure may indirectly threaten civilian survival and well-being. Disruptions to healthcare systems, electricity networks, water supplies, and communication systems may create severe humanitarian consequences even in the absence of immediate physical violence.

For example, a cyber-attack targeting a hospital's computer system could disable life-support equipment, delay medical treatment, or compromise emergency response systems. Such actions may violate the principle of humanity because they expose civilians to unnecessary suffering.

Furthermore, cyber operations targeting critical civilian infrastructure may disproportionately affect vulnerable populations, including children, elderly people, and individuals requiring medical assistance.

The International Committee of the Red Cross has emphasized that states must consider the foreseeable humanitarian consequences of cyber operations and ensure that civilians remain protected during digital

[19] Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon (Crown 2014).

conflict. [20]

Thus, the principle of humanity requires states to conduct cyber operations in a manner that minimizes civilian suffering and preserves essential humanitarian services.

E. State Responsibility

State responsibility is a fundamental principle of international law requiring states to bear legal responsibility for internationally wrongful acts attributable to them. In cyber warfare, determining state responsibility is particularly difficult due to the anonymity and technical complexity of cyber operations.

Attribution refers to identifying the actor responsible for a cyber-attack. States often deny involvement in cyber operations, and attackers frequently conceal their identities through proxy servers, fake digital traces, and third-party infrastructures.

Nevertheless, under international law, states may be held responsible for cyber operations conducted directly by state agencies or by non-state actors operating under state control or support.[21] If a state conducts a cyber operation violating IHL principles, it may incur international responsibility and face legal consequences.

The challenge of attribution significantly complicates accountability mechanisms in cyber warfare. Without reliable attribution, enforcing international law becomes difficult, thereby increasing the risk of impunity for unlawful cyber conduct.

The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations recognizes that existing principles of state responsibility apply to cyber operations, although practical enforcement remains uncertain. [22]

Consequently, strengthening international cooperation, attribution mechanisms, and cyber governance frameworks remain essential for ensuring accountability in cyberspace.

The core principles of International Humanitarian Law; distinction, proportionality, military necessity, humanity, and state responsibility; continue to provide an essential legal framework for regulating cyber warfare. However, applying these principles to cyberspace presents substantial legal and operational challenges due to the interconnected, anonymous, and borderless nature of digital technologies.

While existing IHL rules remain applicable to cyber operations, the evolving character of cyber warfare demonstrates the urgent need for clearer international standards, stronger enforcement mechanisms, and greater international cooperation to protect civilians and preserve humanitarian values in the digital age.

Applicability of International Humanitarian Law to Cyber Warfare

The emergence of cyber warfare has generated intense debate regarding the applicability of International Humanitarian Law (IHL) to cyber operations conducted during armed conflict.

Traditional IHL was primarily developed to regulate conventional warfare involving physical violence, territorial occupation, and kinetic military operations. However, the rapid evolution of cyber capabilities has transformed cyberspace into an important domain of modern conflict, raising fundamental legal questions concerning the adequacy of existing international legal frameworks.

One of the central issues is whether cyber operations may constitute “armed attacks” under international law, thereby triggering the application of IHL and the right of self-defense under the United Nations Charter. Additional concerns involve the applicability of the Geneva Conventions, customary international

[20] https://blogs.icrc.org/law-and-policy/2023/03/07/towards-common-understandings-the-application-of-established-ihl-principles-to-cyber-operations/?utm
[21] https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf?utm
[22] https://ccdcoe.org/research/tallinn-manual/?utm

law, and the interpretation of key legal provisions such as Articles 2(4) and 51 of the UN Charter. In this context, the Tallinn Manual 2.0 on International Law Applicable to Cyber Operations has emerged as one of the most influential scholarly attempts to clarify how international law applies to cyber operations.

This chapter critically evaluates the applicability of IHL to cyber warfare and examines the continuing legal uncertainties surrounding cyber operations.

A. Do Cyber Attacks Qualify as "Armed Attacks"?

One of the most controversial questions in cyber warfare law is whether cyber-attacks can amount to "armed attacks" under international law. The significance of this classification lies in the fact that an armed attack may trigger the inherent right of self-defense recognized under Article 51 of the United Nations Charter. [23]

Traditionally, armed attacks referred to conventional military actions involving physical force, such as bombings, invasions, or missile strikes. However, cyber operations differ significantly because they may cause disruption, economic loss, or infrastructural damage without immediate physical destruction or casualties.

Many scholars argue that cyber operation should qualify as an armed attack if its consequences are comparable to those produced by conventional military forces. For example, a cyber-attack disabling a national electricity grid, contaminating water systems, or causing the explosion of industrial facilities may produce severe humanitarian and economic consequences equivalent to traditional armed attacks.

The Stuxnet operation against Iran's nuclear facilities is often cited as a landmark example.

The malware allegedly damaged Iranian nuclear centrifuges through digital manipulation, causing physical destruction without direct military engagement. [24] This demonstrated that cyber tools could produce kinetic effects traditionally associated with conventional warfare.

Similarly, cyber operations targeting healthcare systems or air traffic control infrastructure could potentially threaten civilian lives on a large scale. Under such circumstances, many legal scholars contend that the threshold of an armed attack would likely be satisfied.

However, significant disagreement remains regarding the precise threshold required for cyber operations to constitute armed attacks. Some states adopt a narrow interpretation requiring physical destruction or casualties, while others favor broader criteria emphasizing scale and effects. This lack of consensus creates legal uncertainty regarding state responses to cyber operations.

The ambiguity surrounding the concept of armed attack demonstrates one of the major weaknesses of current international law in addressing cyber warfare.

B. Applicability of the Geneva Conventions to Cyber Warfare

The four Geneva Conventions of 1949 and their Additional Protocols form the cornerstone of International Humanitarian Law. Although these treaties were drafted before the emergence of modern digital technology, most scholars and international organizations agree that they apply to cyber operations conducted during armed conflict.

The International Committee of the Red Cross has consistently maintained that cyber warfare is not a legal vacuum and that existing IHL rules apply fully to cyber operations during armed conflict. [25]According to

[23] https://www.un.org/en/about-us/un-charter/full-text?utm
[24] Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon (Crown 2014).
[25] https://www.icrc.org/en/document/short-papers-on-international-humanitarian-law-and-cyber-operations-during-armed-conflicts?utm

the ICRC, the principles of distinction, proportionality, military necessity, and humanity remain legally binding regardless of the weapons or technologies employed.

Under the Geneva Conventions, civilians and civilian objects are protected from attack. In cyberspace, this protection extends to civilian digital infrastructure such as hospitals, banking systems, communication networks, and water supply systems. Consequently, cyber-attacks directed against civilian infrastructure may violate IHL if they cause unnecessary suffering or disproportionate harm.

Nevertheless, applying the Geneva Conventions to cyber warfare presents practical difficulties. Unlike conventional weapons, cyber tools often spread unpredictably across interconnected systems. Malware introduced into military networks may unintentionally affect civilian infrastructure beyond the intended target.

Furthermore, modern digital infrastructure frequently serves both civilian and military purposes. Communication satellites, internet providers, and cloud computing systems may support military operations while simultaneously providing civilian services. This dual-use character complicates the principle of distinction and increases the risk of civilian harm.

Another challenge concerns the classification of cyber conflicts themselves. IHL generally applies only during armed conflict, yet many cyber operations occur below the traditional threshold of warfare. Espionage, disinformation campaigns, and economic cyber-attacks may not clearly trigger the full application of IHL despite causing significant disruption.

Therefore, while the Geneva Conventions remain applicable in principle, their practical implementation in cyberspace remains legally complex and operationally uncertain.

C. Customary International Law and Cyber Warfare

In addition to treaty law, customary international law plays a significant role in regulating cyber warfare. Customary international law consists of consistent state practice accompanied by a belief that such practice is legally obligatory (opinion juris).

Because cyber warfare technology has evolved more rapidly than treaty development, customary international law has become particularly important in addressing legal gaps. Many principles governing cyber operations derive not from new treaties but from the adaptation of existing customary norms to cyberspace.

For example, the customary principles of distinction, proportionality, and state responsibility are widely considered applicable to cyber operations. States increasingly acknowledge that cyber activities must comply with international law, even in the absence of a specialized cyber warfare treaty.

However, customary international law in cyberspace remains underdeveloped. State practice regarding cyber operations is often secretive, inconsistent, and politically sensitive. Governments rarely disclose offensive cyber capabilities or publicly acknowledge responsibility for cyber-attacks. As a result, identifying consistent state practice becomes difficult.

Moreover, states frequently disagree regarding the legal interpretation of cyber operations. Some states support expansive interpretations of sovereignty and prohibited intervention in cyberspace, whereas others favor more flexible approaches permitting broader cyber activities.

This fragmentation weakens the clarity and predictability of customary norms governing cyber warfare.

D. United Nations Charter: Article 2(4) and Article 51

The United Nations Charter establishes the foundational legal framework governing the use of force in international relations.

Article 2(4): Prohibition on the Use of Force

Article 2(4) prohibits states from using force against the territorial integrity or political independence of another state. [26] the crucial question in cyber warfare is whether cyber operations constitute "use of force" under this provision.

Most legal scholars argue that cyber operations causing physical destruction or severe societal disruption may qualify as prohibited use of force. For instance, disabling a state's energy grid or causing industrial explosions through cyber means may have consequences comparable to conventional military attacks.

However, not all cyber operations reach this threshold. Cyber espionage, website defacement, or theft of information may violate sovereignty or domestic law without necessarily constituting prohibited uses of force.

The absence of universally accepted criteria for determining when cyber operations amount to force remains one of the most congested areas of international law.

Article 51: Right of Self-Defense

Article 51 recognizes the inherent right of states to self-defense in response to armed attacks.[27] If a cyber operation qualifies as an armed attack, the victim state may lawfully respond through proportionate defensive measures.

However, cyber self-defense raises several complications:

- Difficulty of attribution,
- Uncertainty regarding attack thresholds,
- Risks of escalation,
- Potential for disproportionate responses.

For example, if a state incorrectly attributes a cyber-attack to another state and responds militarily, the consequences could significantly escalate international conflict.

Therefore, while Article 51 theoretically applies to cyber warfare, practical implementation remains highly uncertain.

E. Tallinn Manual 2.0

What Is the Tallinn Manual 2.0?

The Tallinn Manual 2.0 on International Law Applicable to Cyber Operations is a non-binding academic study prepared by an international group of legal experts under the auspices of the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE). Published in 2017, it represents one of the most comprehensive attempts to clarify how existing international law applies to cyber operations. [28]

- The Manual addresses:
- Sovereignty,
- Use of force,
- Armed attacks,
- State responsibility,
- International Humanitarian Law,
- Human rights law,
- Cyber operations during peacetime and armed conflict.

[26] https://www.un.org/en/about-us/un-charter/full-text?utm
[27] https://www.un.org/en/about-us/un-charter/full-text?utm
[28] https://ccdcoe.org/research/tallinn-manual/?utm

Importantly, the Tallinn Manual does not create new laws. Instead, it interprets how existing legal principles apply to cyberspace.

Importance of the Tallinn Manual

The Tallinn Manual has become highly influential in academic, military, and policy discussions concerning cyber warfare. It provides detailed legal analysis and practical guidance for states confronting emerging cyber threats.

Its significance lies in several areas:

1. Clarification of Legal Principles

The Manual helps explain how traditional legal concepts such as sovereignty, use of force, and proportionality may apply to cyber operations.

2. Filling Legal Gaps

In the absence of a comprehensive international cyber treaty, the Manual offers a structured framework for interpreting existing law.

3. Influence on State Practice

Although non-binding, many governments, military institutions, and scholars rely upon the Manual when formulating cyber policies and legal strategies.

4. Contribution to International Debate

The Manual has stimulated global discussion regarding the future development of cyber norms and international law.

Limitations of the Tallinn Manual

Despite its influence, the Tallinn Manual faces substantial criticism.

A. Non-Binding Nature

The Manual is not an international treaty and possesses no legally binding authority. States are not obligated to follow their interpretations.

B. Western-Centric Perspectives

Critics argue that the Manual largely reflects Western legal and strategic viewpoints, particularly those associated with NATO member states. Many non-Western states have not fully endorsed their conclusions.

C. Lack of State Consensus

Numerous legal questions addressed by the Manual remain contested among states. Issues such as sovereignty in cyberspace, thresholds for armed attack, and countermeasures continue to lack universal agreement.

D. Rapid Technological Change

Cyber technologies evolve faster than legal interpretation. Emerging developments involving artificial intelligence, autonomous cyber systems, and quantum computing may exceed the Manual's current framework. Therefore, while the Tallinn Manual provides valuable guidance, it cannot resolve all legal uncertainties associated with cyber warfare.

International Humanitarian Law clearly applies to cyber warfare in principle, yet substantial legal ambiguities remain regarding its practical implementation. Questions surrounding armed attacks, use of force, attribution, civilian protection, and state responsibility continue to challenge traditional legal frameworks.

Although the Geneva Conventions, customary international law, and the UN Charter provide an important legal foundation, cyber warfare exposes significant gaps within existing international law. The Tallinn Manual 2.0 represents a major effort to interpret these rules for cyberspace, but its non-binding nature and lack of universal consensus limit its authority.

Consequently, the growing importance of cyber operations in modern conflict demonstrates the urgent need for clearer international standards, stronger cooperation mechanisms, and the continued evolution of international law in the digital age.

Major Legal Challenges and Gaps in Regulating Cyber Warfare

The rapid expansion of cyber warfare has exposed significant weaknesses within the existing framework of international law. Although International Humanitarian Law (IHL), the United Nations Charter, and customary international law provide a general legal foundation for regulating armed conflict, these rules were primarily developed for conventional warfare rather than cyberspace. Consequently, cyber operations create complex legal uncertainties regarding attribution, accountability, civilian protection, jurisdiction, and enforcement.

Unlike traditional military attacks, cyber operations are often anonymous, transnational, technologically sophisticated, and capable of affecting civilian infrastructure on a massive scale. Moreover, cyber warfare increasingly involves non-state actors operating independently or with covert state support. The absence of a universally binding international cyber treaty further aggravates these challenges.

This chapter critically examines the major legal gaps and operational difficulties associated with regulating cyber warfare under contemporary international law.

A. Attribution Problem

One of the most serious legal obstacles in cyber warfare is the problem of attribution. Attribution refers to identifying the individual, group, or state responsible for conducting a cyber-attack.

In conventional warfare, identifying the attacker is relatively straightforward because military operations are usually conducted openly by identifiable armed forces. In cyberspace, however, attackers can conceal their identity through proxy servers, encrypted communication systems, fake digital footprints, and compromised third-party networks located across multiple jurisdictions.

The attribution problem creates significant legal consequences because international law requires a certain degree of certainty before holding a state internationally responsible for wrongful acts or before exercising the right of self-defense under Article 51 of the United Nations Charter. [29]

For example, during the Russo-Ukrainian War, numerous cyber-attacks targeted Ukrainian government institutions, banking systems, media outlets, and communication networks. Although many governments and cybersecurity experts attributed several of these attacks to Russian-affiliated actors, direct legal proof linking the operations to the Russian state remained difficult to establish publicly. [30]

Similarly, the 2007 cyber-attacks against Estonia severely disrupted governmental and financial systems through large-scale Distributed Denial-of-Service (DDoS) attacks. Estonia accused Russia of involvement, yet conclusive legal attribution remained challenging due to the decentralized and anonymous nature of the attacks. [31]

[29] https://www.un.org/en/about-us/un-charter/full-text?utm
[30] https://www.cfr.org/in-brief/how-russia-ukraine-conflict-shaping-future-cyberwarfare?utm
[31] https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf?utm

The inability to accurately identify perpetrators creates several problems:

- Difficulty in enforcing state responsibility,
- Obstacles to lawful countermeasures,
- Increased risk of wrongful retaliation,
- Weak accountability mechanisms,
- Greater opportunity for impunity.

Moreover, states may intentionally exploit attribution uncertainty by conducting cyber operations through proxy groups or unofficial actors, thereby avoiding direct legal responsibility.

The attribution problem therefore remains one of the greatest weaknesses in applying international law to cyber warfare.

B. Anonymous Nature of Cyber Attacks

Closely connected to attribution is the inherently anonymous nature of cyber operations. Cyber-attacks can often be conducted remotely from virtually any location in the world without physical presence within the target state.

- Attackers frequently use:
- Virtual private networks (VPNs),
- Botnets,
- Encrypted communication,
- Fake IP addresses,
- Third-party servers,

Malware is designed to erase digital traces.

This anonymity creates substantial legal and security challenges because victims may not immediately known:

- Who launched the attack,
- Whether the attack was state-sponsored,
- Whether the operation constitutes espionage, cybercrime, or armed conflict,
- Whether the attack threshold justifies self-defense.

For instance, ransomware groups may operate independently while simultaneously receiving indirect protection or support from states unwilling to prosecute them. This blurring of lines between criminal activity and state-sponsored cyber operations complicates international legal responses.

The WannaCry ransomware attack in 2017 affected more than 150 countries, targeting hospitals, transportation systems, businesses, and public institutions. [32] Although the United States and several allies later attributed the attack to actors associated with North Korea, the anonymous nature of the operation initially complicated international response efforts.

Anonymity also increases the risk of escalation in international relations. Incorrect attribution may lead states to retaliate against the wrong actor, potentially intensifying political or military tensions.

Furthermore, anonymity weakens deterrence because attackers often believe they can avoid accountability. As a result, cyber warfare creates a strategic environment where hostile operations may occur below the threshold of traditional armed conflict without immediate legal consequences.

C. Civilian Infrastructure Vulnerability

One of the most alarming features of cyber warfare is the vulnerability of civilian infrastructure. Modern

[32] https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst?utm

societies depend heavily on interconnected digital systems controlling essential public services such as healthcare, banking, electricity, transportation, and water supply.

Under International Humanitarian Law, civilians and civilian objects enjoy protection during armed conflict. However, cyber warfare creates unique risks because civilian and military systems are frequently interconnected through shared digital infrastructure.

1. Hospitals and Healthcare Systems

Hospitals and medical facilities are among the most sensitive civilian targets in cyberspace. Cyber-attacks against healthcare systems may disable life-support equipment, delay emergency treatment, compromise patient records, and disrupt public health services.

The International Committee of the Red Cross has repeatedly warned that cyber-attacks against healthcare infrastructure can create severe humanitarian consequences. [33]

During the COVID-19 pandemic, several healthcare institutions worldwide became targets of ransomware attacks, demonstrating the vulnerability of medical systems during crises.

Similarly, cyber operations affecting Ukrainian healthcare infrastructure during the ongoing conflict raised concerns regarding civilian protection under IHL.

A hospital's computer network would generally constitute a protected civilian object under international law unless it is being used directly for military purposes. Nevertheless, distinguishing between civilian and military cyber infrastructure remains highly difficult in practice.

2. Banking and Financial Systems

Modern financial systems rely extensively on digital networks. Cyber-attacks targeting banking institutions can disrupt national economies, freeze financial transactions, undermine public confidence, and create widespread economic instability.

Cyber operations against financial infrastructure may produce indirect humanitarian consequences by affecting salaries, emergency funding, food distribution systems, and public services.

For example, cyber-attacks against Ukrainian banking systems during the Russia–Ukraine conflict disrupted financial services and increased economic uncertainty. [34] Such operations demonstrate how cyber warfare can destabilize civilian life without direct physical violence.

The challenge for international law lies in determining whether attacks on financial systems constitute unlawful uses of force or armed attacks under the UN Charter.

3. Power Grids and Energy Infrastructure

Energy infrastructure represents one of the most strategically important and vulnerable sectors in cyber warfare.

Cyber-attacks targeting electricity grids can:

- Disable hospitals,
- Interrupt water supply,
- Disrupt transportation,
- Affect communication systems,
- Endanger civilian populations during extreme weather conditions.

One notable example occurred in Ukraine in 2015 and 2016 when cyber-attacks disrupted portions of the country's electricity grid, leaving thousands of civilians without power. [35] These incidents illustrated how

[33] https://www.icrc.org/en/document/cyber-attack-health-care?utm
[34] https://www.weforum.org/stories/2022/03/cyberwarfare-ukraine-russia-explainer/?utm
[35] https://www.csis.org/analysis/cyberattack-against-ukrainian-power-grid?utm

cyber operations could produce significant societal disruption comparable to conventional attacks.
Because critical civilian infrastructure often supports both civilian and military functions, applying the principle of distinction becomes extremely difficult.
The vulnerability of civilian infrastructure therefore exposes one of the major humanitarian gaps within current cyber warfare regulations.

D. Non-State Actors

Another major challenge concerns the growing role of non-state actors in cyber warfare.
Traditionally, international law primarily regulated the conduct of sovereign states. However, cyberspace enables private individuals, terrorist groups, hacktivists, criminal organizations, and proxy militias to conduct cyber operations with significant international consequences.
Non-state actors possess several advantages:

- Low operational costs,
- Global reach,
- Relative anonymity,
- Access to sophisticated malware tools,
- Ability to operate across borders.

Some groups conduct politically motivated cyber-attacks independently, while others may operate with covert support from states seeking plausible deniability.
For example, several cyber operations during the Russia–Ukraine conflict involved hacker collectives and volunteer cyber groups supporting either side. [36] These actors have complicated questions regarding combatant status, accountability, and state responsibility.
International law struggles to address non-state cyber actors because:

- Existing treaties primarily regulate states,
- Attribution remains difficult,
- Jurisdictional enforcement is weak,
- Non-state actors frequently operate transnationally.

The increasing involvement of non-state actors therefore undermines the traditional state-centric structure of international law.

E. Jurisdictional Problems

Cyber warfare creates substantial jurisdictional complications because cyber operations frequently cross multiple territorial boundaries simultaneously.

- A single cyber-attack may involve:
- An attacker located in one state,
- Servers located in several other states,
- Victims located globally,
- Financial transactions are routed through additional jurisdictions.

This creates uncertainty regarding:

- Which state possesses legal authority,
- Which laws apply,
- How evidence should be collected,

[36] https://www.nato.int/docu/review/articles/2023/05/16/ukraine-and-the-future-of-cyber-war/index.html?utm

- How international cooperation should occur.

Different states also maintain different domestic cyber laws, enforcement standards, and interpretations of sovereignty in cyberspace.

For example, some states consider unauthorized cyber intrusion alone a violation of sovereignty, whereas others require significant physical or functional damage before recognizing international legal violations.

Jurisdictional fragmentation creates enforcement gaps because cyber criminals or hostile actors may exploit states with weak cyber governance systems or limited law enforcement capacity.

Furthermore, extradition and mutual legal assistance processes often remain too slow for rapidly evolving cyber incidents.

Consequently, cyber warfare demonstrates the limitations of territorially based legal systems in addressing borderless digital conflict.

F. Lack of a Binding International Cyber Treaty

Perhaps the most significant legal gap in cyber warfare regulation is the absence of a comprehensive and universally binding international treaty specifically governing cyber operations during armed conflict.Although existing international law applies in principle, there is currently no dedicated treaty clearly defining:

- Cyber warfare,
- Armed attack thresholds,
- State responsibilities,
- Civilian cyber protection,
- Attribution standards,
- Enforcement mechanisms.

The Tallinn Manual 2.0 on International Law Applicable to Cyber Operations provides influential legal guidance, but it is non-binding and reflects expert opinion rather than universally accepted law. [37]

Similarly, United Nations discussions on cyber norms and responsible state behavior have produced limited consensus. Major geopolitical rivalries between technologically advanced states continue to obstruct the development of binding international rules.

The absence of a binding treaty creates several risks:

- Legal uncertainty,
- Inconsistent state practices,
- Weak accountability,
- Increased risk of escalation,
- Insufficient civilian protection.

Without clearer legal standards, states may interpret cyber rules differently according to political or strategic interests. Therefore, many scholars and international organizations increasingly advocate for the development of stronger international cyber governance frameworks or a specialized “Digital Geneva Convention” capable of addressing contemporary cyber threats.

Cyber warfare exposes profound legal and institutional weaknesses within the current international legal order.

Problems relating to attribution, anonymity, civilian vulnerability, non-state actors, jurisdiction, and the absence of binding treaty law significantly complicate the regulation of cyber operations.

[37] https://ccdcoe.org/research/tallinn-manual/?utm

The Russia–Ukraine cyber incidents, attacks on healthcare systems, and disruptions to critical infrastructure demonstrate that cyber warfare poses serious threats not only to national security but also to humanitarian protection and global stability.

Although International Humanitarian Law and the UN Charter continue to provide an important legal foundation, existing frameworks remain insufficiently adapted to the realities of modern cyber conflict. Addressing these challenges requires stronger international cooperation, clearer legal standards, improved attribution mechanisms, and the gradual development of binding international cyber norms.

Case Studies and Contemporary Examples

A. Stuxnet Attack (Iran)

One of the most significant examples of cyber warfare is the Stuxnet attack discovered in 2010, which targeted Iran's nuclear enrichment facilities at Natanz. The malware was specifically designed to infiltrate industrial control systems and manipulate uranium enrichment centrifuges, causing physical damage while disguising the malfunction from operators. [38] The operation is widely believed to have been conducted through cooperation between the United States and Israel, although neither state officially acknowledged responsibility. [39]

The Stuxnet incident marked a turning point in the evolution of cyber warfare because it demonstrated that cyber operations could produce physical destruction traditionally associated with conventional military attacks. Unlike ordinary cybercrime or espionage, the attack directly damaged critical infrastructure through malicious code. This significantly expanded the understanding of cyberspace as a domain capable of supporting offensive military operations.

Legally, the attack raised important questions regarding attribution, sovereignty, and the threshold of "armed attack" under international law. Scholars continue to debate whether Stuxnet constituted unlawful use of force under Article 2(4) of the United Nations Charter or whether it could justify self-defense under Article 51.

B. Russia–Ukraine Cyber Conflict

The ongoing Russo-Ukrainian War represents one of the clearest modern examples of the integration of cyber operations into conventional warfare. Since the escalation of the conflict in 2022, Ukraine has experienced numerous cyber-attacks targeting governmental institutions, banking systems, communication networks, and energy infrastructure. [40]

Cyber-attacks against Ukrainian electricity grids disrupted civilian services and demonstrated the vulnerability of critical infrastructure during armed conflict. Banking systems and communication services were also affected, creating economic instability and public disruption. [41] These incidents illustrate how cyber operations can affect civilian populations even when military objectives are pursued.

The Russia–Ukraine conflict also exposed major legal challenges in applying traditional International Humanitarian Law to cyberspace. Determining attribution, distinguishing military from civilian targets, and assessing proportionality remain highly difficult due to the interconnected nature of digital infrastructure.

[38] Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon (Crown 2014).
[39] https://www.britannica.com/technology/Stuxnet?utm
[40] https://www.cfr.org/in-brief/how-russia-ukraine-conflict-shaping-future-cyberwarfare?utm
[41] https://www.weforum.org/stories/2022/03/cyberwarfare-ukraine-russia-explainer/?utm

These incidents demonstrate that cyber operations can produce humanitarian consequences similar to conventional warfare while remaining legally ambiguous under current international law.

Recommendations and Legal Reforms

The growing use of cyber operations in modern conflicts demonstrates that existing international legal frameworks remain insufficient to address the complex realities of digital warfare. Although International Humanitarian Law (IHL) provides important foundational principles, significant legal ambiguities continue to exist regarding attribution, civilian protection, state responsibility, and enforcement mechanisms in cyberspace. Consequently, stronger legal reforms and international cooperation are essential for ensuring accountability and humanitarian protection in the digital age.

1. Development of an International Cyber Warfare Treaty

The international community should develop a comprehensive and legally binding treaty specifically regulating cyber warfare.

Such a treaty should establish uniform rules concerning cyber operations during armed conflict, prohibited targets, state obligations, and accountability mechanisms. Existing frameworks rely heavily on interpretation rather than explicit regulation, creating uncertainty and inconsistent state practices.

2. Clear Definition of "Cyber Attack" and "Armed Attack"

International law currently lacks universally accepted definitions of cyber-attack and armed attack in cyberspace. Clear legal definitions are necessary to determine when cyber operations constitute unlawful uses of force or trigger the right of self-defense under Article 51 of the United Nations Charter. [42]

3. Stronger Protection of Civilian Infrastructure

Critical civilian infrastructure such as hospitals, banking systems, water facilities, and electricity grids should receive enhanced legal protection from cyber operations. International legal standards should explicitly prohibit cyber-attacks targeting essential humanitarian services that may endanger civilian lives.[43]

4. Improved Attribution Mechanisms

The international community should establish more effective technical and legal mechanisms for cyber attribution. Reliable attribution is essential for ensuring accountability, preventing wrongful retaliation, and enforcing state responsibility under international law.

5. Greater International Cooperation and Intelligence Sharing

Cyber threats are transnational in nature and therefore require stronger international cooperation. States should increase intelligence sharing, cybersecurity coordination, and collaborative investigations through international organizations and regional partnerships.

6. Capacity Building for Developing Countries

Developing countries such as Bangladesh often lack adequate technological infrastructure, cybersecurity expertise, and legal preparedness to respond effectively to cyber threats. International assistance programs should therefore support capacity building, legal development, and cyber defense training for vulnerable states.

[42] https://www.weforum.org/stories/2022/03/cyberwarfare-ukraine-russia-explainer/?utm
[43] https://www.icrc.org/en/document/short-papers-on-international-humanitarian-law-and-cyber-operations-during-armed-conflicts?utm

Existing humanitarian principles alone are insufficient without specialized legal mechanisms tailored to cyberspace. The evolving nature of cyber warfare requires the continuous adaptation of international law to ensure effective civilian protection, state accountability, and global cyber stability.

Conclusion

Cyber warfare has emerged as one of the most significant challenges confronting contemporary international law and global security. The rapid expansion of digital technologies and the increasing dependence of states on cyberspace have transformed cyber operations into powerful tools capable of disrupting critical infrastructure, governmental systems, military operations, and civilian life. Incidents such as the Stuxnet attack and the cyber operations associated with the Russo-Ukrainian War demonstrate that cyber-attacks can produce consequences comparable to conventional warfare, including physical destruction, economic instability, and humanitarian suffering.[44] At the same time, the anonymous and transnational nature of cyber operations creates serious legal and operational difficulties for the international community.

This study finds that the core principles of International Humanitarian Law (IHL), including distinction, proportionality, military necessity, humanity, and state responsibility, remain applicable to cyber warfare in principle. Existing legal frameworks such as the Geneva Conventions, customary international law, and the United Nations Charter provide an important legal foundation for regulating cyber operations during armed conflict.[45] However, significant legal gaps continue to exist regarding attribution, armed attack thresholds, civilian infrastructure protection, non-state actors, and enforcement mechanisms. The absence of a comprehensive and binding international cyber warfare treaty further contributes to legal uncertainty and inconsistent state practice.

Therefore, international law must continue evolving alongside technological developments to ensure meaningful humanitarian protection in cyberspace. Stronger international cooperation, clearer legal standards, improved attribution systems, and specialized cyber governance mechanisms are essential for addressing emerging cyber threats effectively.

As warfare increasingly shifts from battlefields to digital networks, the survival of humanitarian protection will depend upon the international community's ability to modernize legal frameworks for cyberspace.

[44] https://www.icrc.org/en/document/short-papers-on-international-humanitarian-law-and-cyber-operations-during-armed-conflicts?utm

[45] https://www.un.org/en/about-us/un-charter/full-text?utm