IPRI Islamabad Policy Research Institute
Research | Innovation | Dialogue | Policy

POLICY BRIEF

The Digital Battlefield: Regulating Cyber Warfare in International Law

Iqra Bano Sohail
Naimat Khan Jaffar

May 2025

Chair International Law

Executive Summary

Cyber warfare has emerged as a prominent method for states to pursue strategic objectives by targeting digital infrastructure, disrupting essential services, and spreading disinformation, all without engaging in traditional military action. These operations often evade attribution and accountability, complicating legal responses and blurring the boundaries of what constitutes as the use of force under international law. Despite the growing frequency and impact of such incidents, international legal frameworks like the UN Charter and International Humanitarian Law (IHL) offer limited guidance on how to classify or respond to cyberattacks. Additionally, the lack of a shared definition and legal clarity leaves room for interpretation and exploitation. To address this, the international community must prioritize the development of common norms, improve legal mechanisms for accountability, and ensure that protections for civilians and critical systems are upheld in the digital realm.

Policy Recommendations

- The United Nations (UN) and international legal bodies should define cyber warfare to enhance legal clarity and deterrence. The definition should cover state attributed malicious cyber operations targeting critical infrastructure with coercive intent and significant impact.
- ICRC should issue official commentaries that address challenges unique to cyberspace, such as the interconnectedness of civilian and military systems, the risk of indiscriminate effects, and the attribution of cyber operations to parties in conflict.
- States should establish a cyber weapons review process based on Article 36 of Additional Protocol I to the Geneva Conventions to ensure new cyber tools comply with IHL. This includes assessing their potential impact, legality, and risks to civilians before deployment.
- Regional cyber security alliances such as the Association of Southeast Asian Nations (ASEAN) should be promoted to enhance collective resilience against cross-border cyber threats. These alliances can focus on joint threat assessments and capacity building through training programs fostering cooperation among member states.

INTRODUCTION

The nature of warfare has expanded far beyond traditional battlefields. In today's interconnected world, cyberspace has become a contested arena where wars are fought with malware, ransom ware, and data breaches. Cyber warfare allows adversaries to inflict strategic damage by targeting essential systems such as power infrastructure, financial institutions, healthcare networks, and democratic process.[1] The invisible and often anonymous nature of cyberattacks makes them particularly dangerous, as attribution is difficult and accountability is rare.

Despite the increasing scale and severity of cyber threats, international legal institutions struggle to define the parameters of cyber conflict, let alone regulate it effectively. Current frameworks such as the United Nations Charter and International Humanitarian Law (IHL) offer limited applicability, and there is a pressing need to establish clear norms that address the realities of this threat.

Recent developments, such as Pakistan's cyber operations against India focused only on military targets.[2] This stance underscores the importance of distinguishing lawful military cyber operations from indiscriminate attacks on civilian infrastructure. This is because that a targeted attack against a military target which does not have any civilian fall out but cripples a military communication system does not violate any principle of IHL.

This reality challenges how cyber warfare is defined and regulated. Engaging in cyber attacks compels a reconsideration of the parameters of cyber conflict, emphasizing the need for definitions that account for both offensive and defensive state actions.

UNDERSTANDING CYBER WARFARE

Cyber warfare refers to hostile actions carried out in cyberspace with the intent to disrupt, damage, or gain unauthorized access to another state's critical systems or information networks.[3] Unlike traditional armed conflicts, these operations do not rely on physical force

[1]Hathaway, Oona A., et al. "The Law of Cyber-Attack." *California Law Review*, vol. 100, no. 4, pp. 817-886. https://openyls.law.yale.edu/bitstream/handle/20.500.13051/3283/Law_of_Cyber.pdf accessed March 04, 2025

[2] 'Operation Bunyan-ul-Marsoos key Indian military and cyber targets hit by Pakistan' The Nation (Islamabad, 10 May 2025) https://www.nation.com.pk/10-May-2025/operation-bunyan-ul-marsoos-key-indian-military-and-cyber-targets-hit-by-pakistan accessed 15 May 2025.

[3] ibid

but can produce damaging consequences, including economic destabilization, social unrest, and even loss of life through the disruption of essential services. Despite its growing prevalence, there remains no universally accepted definition of cyber warfare, which complicates efforts to regulate such activities and hold perpetrators accountable under international law.

It is essential to differentiate between various forms of malicious cyber activity. While the term "cyber attacks" serves as an umbrella for acts such as espionage, data theft, and system disruptions, carried out by individuals, criminal syndicates, or state actors, cyber warfare typically refers to operations orchestrated or sponsored by states with defined military or political objectives. These operations often coincide with, or precipitate, armed conflicts. Instances such as disabling national power grids or sabotaging military communications exemplify the strategic nature of cyber warfare. In contrast, cybercrime remains financially motivated, targeting individuals or corporations for illicit gain through tactics such as phishing or identity theft.[4]

Various scholars and states have attempted to define cyber warfare, reflecting differing perspectives on its scope and nature. Laurent Gisel, Legal Advisor at the International Committee of the Red Cross, frames cyber warfare as cyber operations conducted within the context of an armed conflict under IHL, emphasizing the need for legal boundaries around such activities.[5] Richard Clarke defines cyber war as, "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption".[6]

States also vary in their approach. The United States, United Kingdom, Russia, China, Israel, Iran, and North Korea have developed offensive and defensive cyber capabilities, reflecting their recognition of cyber operations as integral to national security and warfare. For instance, the US Department of Defense defines cyber warfare as politically motivated computer hacking aimed at sabotage and espionage, analogous to traditional armed conflict[7].

---

[4] Haroon, S, *International Humanitarian Law on Cyberwarfare and Pakistan's Legal Framework* (Research Society of International Law, September 2015).

[5] 'What is Cyber Warfare?' American Public University https://www.apu.apus.edu/area-of-study/information-technology/resources/what-is-cyber-warfare/#:~:text=cyber%20warfare%20is%20means%20and%20methods%20of%20warfare

[6] Richard A Clarke, and Robert K. Knake, Cyber war (New York: Tantor Media Incorporated, 2014), 10.

[7] Ashraf, C., 'Defining cyberwar: towards a definitional framework' (2021) 37(3) *Defense & Security Analysis* 274.

A key definitional challenge remains whether cyber warfare only occurs during an armed conflict or if standalone cyber attacks can constitute cyber warfare. Many experts argue that cyber warfare should meet a threshold of severity akin to an armed attack under Article 51 of the UN Charter to justify self-defense, while lesser cyber incidents may be categorized as cybercrime or espionage. This threshold-based approach is critical, as it underpins the development of effective regulatory frameworks.[8]

In recent years, the frequency and sophistication of cyber operations have increased significantly. In 2015, Russia conducted a cyberattack on Ukraine's power grid, leaving thousands without electricity[9]. One of the most notable examples is the Stuxnet virus, developed by the United States and Israel, which successfully sabotaged Iran's nuclear centrifuges without the use of conventional weaponry.[10] These cases illustrate how cyber warfare has become a powerful instrument of statecraft, capable of achieving strategic goals without engaging in direct military confrontation.

Tactics and Tools of Modern Cyber Warfare

Cyber warfare is conducted through an array of sophisticated digital strategies that enable both state and non-state actors to infiltrate, disrupt, and manipulate adversary networks. At the heart of these operations lies the deployment of malware, including viruses, worms, and ransom ware, which infect systems to extract sensitive data. Another widespread method is phishing, often combined with social engineering, which exploits human behavior to trick individuals into revealing confidential information.

More advanced tactics include Distributed Denial of Service (DDoS) attacks, which flood servers and networks with traffic to render them inaccessible. Additionally, cyber espionage has become a dominant tool for intelligence gathering, where actors, often backed by states, breach classified systems to extract sensitive information. [11]

---

[8] ibid

[9] Greenberg, A. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday. Retrieved from https://books.google.com/books/about/Sandworm.html?id=ujxrDwAAQBAJ

[10] Verton, D. (2021). Stuxnet explained: The first known cyberweapon. https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

[11] Hathaway, Oona A., et al. "The Law of Cyber-Attack." *California Law Review*, vol. 100, no. 4, pp. 817-886. https://openyls.law.yale.edu/bitstream/handle/20.500.13051/3283/Law_of_Cyber.pdf accessed March 04,2025

AN INTERNATIONAL LAW PERSPECTIVE

The UN Charter and the Use of Force in Cyberspace

The Charter of the United Nations (1945) articulates the fundamental principles governing the use of force in international relations. However, the application of these principles to cyber operations remains a complex and unsettled area of international law.

Article 2(4) of the UN Charter provides that

> *"All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."*

This provision, while traditionally interpreted to prohibit physical military action, does not expressly limit its scope to armed or physical force. The phrase "use of force" is sufficiently broad to encompass actions that result in severe disruption or damage to a state's critical infrastructure[12]. While cyber operations do not involve physical weaponry, they can nonetheless undermine a state's political independence or territorial integrity. Consequently, many legal scholars argue that where a cyberattack produces consequences analogous to a physical force, it may fall within the ambit of Article 2(4), particularly if it targets core state functions.

Furthermore, article 39 empowers the United Nations Security Council (UNSC) to "*determine the existence of any threat to the peace, breach of the peace, or act of aggression,* "and to take appropriate collective measures. This provision grants the Council wide discretion in assessing threats to international peace and security. However, despite the increasing prevalence of state-sponsored cyber operations, no cyberattack has yet been officially categorized by the Security Council as a "threat to the peace" or an "act of aggression" under Article 39. The absence of such recognition underscores the legal and political uncertainty surrounding the classification of cyber warfare. [13]

---

[12] Justia, 'Use of Force Under International Law' https://www.justia.com/international-law/use-of-force-under-international-law/ accessed 01 April 2025.

[13] Protecting critical infrastructures against malicious cyber operations: A role for international law?' https://www.law.kuleuven.be/citip/blog/protecting-critical-infrastructures-against-malicious-cyber-operations-a-role-for-international-law/

Nevertheless, a cyber operation that disables critical infrastructure or endangers civilian populations could constitute a threat to international peace within the meaning of Article 39, thereby falling under the Council's jurisdiction. The lack of precedent, however, continues to inhibit the development of binding international norms in this area.

Tallinn Manual 2.0[14]

The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations stands as the most comprehensive non-binding legal analysis to date, offering an interpretation of how traditional principles of international law apply in the cyber context. Developed by the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE), the manual aims to provide interpretative guidance on state conduct in cyberspace, with a particular focus on issues of sovereignty, use of force, armed conflict, and state responsibility.

One of the Manual's key contributions is its interpretation of Article 51 of the UN Charter, which guarantees the inherent right of self-defense in the event of an "armed attack." The Tallinn Manual asserts that under certain circumstances cyber operations can rise to the level of an armed attack if they lead to consequences akin to those of physical warfare. In such instances, a state affected by a cyber operation may invoke the right to individual or collective self-defense.

Sovereignty[15] is another core principle addressed in the Tallinn Manual 2.0. The Manual asserts that states must refrain from allowing their territory, whether physical or digital, to be used for cyber operations that negatively impact the rights of other states. This principle has sparked considerable legal debate, particularly with regard to the permissibility of countermeasures or preemptive cyber operations within another state's digital infrastructure. The unsettled nature of these debates highlights the broader tension between the principles of sovereignty and the practical need for attribution and deterrence in the cyber realm.

International Humanitarian Law (IHL)

Cyber warfare has the capability to violate various foundational principles of IHL. It can be argued that a targeted attack against a military target which does not have any civilian fall out but cripples a military communication system should not violate any principle of IHL.

---

[14] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf

[15] Jus Corpus, 'TERRITORIAL SOVEREIGNTY IN CYBERSPACE & CYBERESPIONAGE' https://www.juscorpus.com/territorial-sovereignty-in-cyberspace-cyberespionage/

Principle of Distinction

The principle of distinction[16] mandates that parties in conflict must differentiate between combatants and civilians, ensuring that military operations avoid harm to non-combatants. However, cyberattacks frequently lack precision and may inadvertently target civilian infrastructure. A notable example is the 2017 NotPetya cyberattack[17], which disrupted Ukrainian banks, hospitals, and government agencies, causing significant economic and social damage.

Principle of Proportionality

The principle of proportionality[18] asserts that any attack must not cause collateral damage that exceeds the anticipated military benefit. Cyberattacks, however, are often difficult to control and can have unforeseen and disproportionate outcomes. For instance, the Stuxnet[19] virus inadvertently spread beyond its target, infecting thousands of civilian computers worldwide.

Principle of Military Necessity

The principle of military necessity[20] dictates that military actions should only serve a legitimate military objective. However, as evident from the above examples, many cyberattacks are executed for purposes such as political coercion, or economic sabotage.

OPTIONS FOR THE INTERNATIONAL COMMUNITY

The Need for a Universal Definition

The establishment of a universally accepted definition of cyber warfare is imperative for enhancing legal clarity, enabling the formulation of effective deterrence mechanisms, and

[16] 15 Article 48 of the 1977 Additional Protocol I to the Geneva Convention
[17] Zoho Workplace, 'The NotPetya Cyberattack: A Detailed Look' https://www.zoho.com/workplace/articles/notpetya-cyberattack.html
[18] 16 Article 51(5)(b) of the 1977 Additional Protocol I Geneva Convention
[19] Verton, D. (2021). Stuxnet explained: The first known cyberweapon. https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html
[20] Princinple of *Proportionality*. Guide to International Humanitarian Law https://guide-humanitarian-law.org/content/article/3/proportionality/

ensuring accountability. Notably, the current absence of such a definition creates space for states and non-state actors to exploit cyber capabilities without clear consequences. [21]

A comprehensive and robust definition of cyber warfare should incorporate several essential elements to ensure both conceptual clarity and practical applicability. First, it must address the nature of the action, explicitly identifying malicious intent as a key characteristic. Malicious intent in this context should reflect the deliberate use of cyber tools to disrupt, damage, or destroy information systems, networks, or data. Furthermore, attribution is another critical factor, hence the action must be traceable to a state, either directly or through actors operating under its control. This distinction is vital to distinguish cyber warfare from mere criminal or hacker activities.

Secondly, the definition should account for the target and scale of the impact. Cyber operations that affect critical national infrastructure, military assets, or essential services should fall within the scope of cyber warfare, particularly where such operations result in significant disruption.

Finally, the purpose and objective of the cyber operation should reflect a coercive intent aligned with strategic military, political, or economic goals. The use of such operations as instruments of statecraft, intended to intimidate or compel another state to act or refrain from acting in a certain manner, reinforces their classification as acts of warfare. [22]

The International Committee of the Red Cross (ICRC) to Issue Commentaries

As the guardian of the Geneva Conventions, ICRC plays a crucial role in ensuring that IHL remains relevant in the face of evolving threats. These commentaries would provide essential legal clarity, reinforce humanitarian principles, and guide states in adapting their national frameworks to address this emerging challenge.[23]

Given the increasing use of cyber tools in armed conflicts, the ICRC should emphasize that IHL applies fully to cyber operations just as it does to traditional weapons and methods of warfare, regardless of the novel and technical nature of cyberspace. The commentaries should also address challenges unique to cyberspace, such as the interconnectedness of civilian and

[21] Bush Center, 'Cyber Warware' https://www.bushcenter.org/catalyst/modern-military/sciarrone-cyber-warfware
[22] TechTarget, 'cyberwarfare' https://www.techtarget.com/searchsecurity/definition/cyberwarfare
[23] ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts (ICRC, 2019)

military systems, the risk of indiscriminate effects, and the attribution of cyber operations to parties in conflict.

By providing clear legal guidance on these issues, the ICRC can help states adapt their national frameworks and military practices to ensure compliance with IHL in the cyber domain, thereby reinforcing humanitarian protections amid evolving threats.

Establishing a Weapons Review Process for emerging Cyber Tools

The implementation of a weapons review process for cyber capabilities, modeled on the principles outlined in Article 36 of Additional Protocol I to the Geneva Conventions, is essential to ensure that cyber tools and techniques used in warfare are consistent with the core tenets of IHL.[24] Article 36 mandates that states evaluate the legality of new weapons and means of warfare before deploying them, ensuring they do not breach IHL principles. Given the increasingly prominent role of cyber operations in modern conflict, it is crucial that similar legal safeguards are applied to cyber capabilities to ensure they do not undermine the protections afforded by IHL.

To effectively adapt this process to the realm of cyber warfare, states must establish mechanisms to review both existing and new cyber tools before they are used in military operations. This weapons review process would involve evaluating the potential impact of a cyber tool, both on the battlefield and in the wider societal context. Just as conventional weapons, cyber tools should also undergo a legal and technical assessment to ensure they do not inadvertently violate the principles that govern warfare.[25]

Promote Regional Cyber Security Alliances

Promoting regional cyber security alliances is essential to fostering collective resilience against the growing threat of cross-border cyber attacks. Regional alliances such as the European Union (EU), the Association of Southeast Asian Nations (ASEAN), and similar groupings are uniquely positioned to enhance cybersecurity cooperation through shared geographical, political, and economic interests.[26]

---

[24] https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0902.pdf
[25] CCDCOE Wiki, 'Legal review of cyber weapons, means and methods of warfare' https://cyberlaw.ccdcoe.org/wiki/Legal_review_of_cyber_weapons,_means_and_methods_of_warfare
[26] UNIDIR, The Role of Regional Organizations in Strengthening Cybersecurity and Stability: Experiences and Opportunities (2020) https://unidir.org/files/publication/pdfs/the-role-of-regional-organizations-in-strengthening-cybersecurity-and-stability-experiences-and-opportunities-en-789.pdf

Such cooperation should include the development of joint threat assessment mechanisms and regional situational awareness platforms. Regional alliances can also play a vital role in capacity building by organizing regular training programs or workshops tailored to local contexts and emerging threats. These joint initiatives would not only enhance the technical proficiency of national cybersecurity agencies but also promote interoperability and mutual trust among member states.

POLICY RECOMMENDATIONS

- The United Nations and international legal bodies should define cyber warfare to enhance legal clarity and deterrence. The definition should cover state attributed malicious cyber operations targeting critical infrastructure with coercive intent and significant impact.
- ICRC should issue official commentaries that address challenges unique to cyberspace, such as the interconnectedness of civilian and military systems, the risk of indiscriminate effects, and the attribution of cyber operations to parties in conflict.
- States should establish a cyber weapons review process based on Article 36 of Additional Protocol I to the Geneva Conventions to ensure new cyber tools comply with IHL. This includes assessing their potential impact, legality, and risks to civilians before deployment. Such reviews would promote accountability and prevent unlawful cyber warfare.
- Regional cyber security alliances such as ASEAN should be promoted to enhance collective resilience against cross-border cyber threats. These alliances can focus on joint threat assessments and capacity building through training programs fostering cooperation among member states.

Action Matrix				
Options for International Community				
Option	**Pathways to Solution**	**Implementation of Solution**	**Actors Responsible**	**Implementation Timelines**
The Need for a Standardized Definition	The establishment of a universally accepted definition of cyber warfare is imperative for enhancing legal clarity, enabling the formulation of effective deterrence mechanisms, and ensuring accountability in the rapidly evolving domain of digital conflict	Convene global discussions under UN bodies, such as the UN General Assembly (UNGA) and the UN Interregional Crime and Justice Research Institute (UNICRI), to develop a comprehensive and legally recognized definition.	• United Nations General Assembly • United Nations Interregional Crime and Justice Research Institute	3-6 Months for Initial consultations among international organizations and legal experts to draft a standardized definition. 3-6 Months for multilateral negotiations to refine and finalize the definition. 6-12 Months for adoption of the definition through international agreements or resolutions.
ICRC Commentaries on challenges unique to cyberwarfare	These commentaries would provide essential legal clarity, reinforce humanitarian principles, and guide states in adapting their national frameworks to address this emerging challenge	The ICRC will conduct legal assessments, engage with international legal experts, and publish authoritative commentaries to guide states and military institutions.	• International Committee of the Red Cross • UN Office of the High Commissioner for Human Rights	12-18 Months for drafting, review, publication and dissemination of commentaries
Establishing a Weapons Review Process for Cyber Tools	Develop a standardized process for reviewing cyber capabilities under IHL principles. Align with existing military directives and conduct legal and technical evaluations of cyber tools' effects.	Integrate legal reviews into the acquisition lifecycle, requiring assessments of cyber tools compliance with IHL. Conduct exercises to test compliance and ensure transparency in legal findings.	• International Committee of the Red Cross (ICRC) • UN Office for Disarmament Affairs	6-12 Months for policy drafting and framework adoption.
Promoting Regional Cyber Security Alliances	Create regional platforms and develop structured information sharing arrangements among member states. Organize regular training programs	Establish standardized reporting formats for cross-border incidents.	• Regional alliances (e.g., EU, ASEAN, AU) • International Telecommunica	6-12 Months for platform development and member-state onboarding.

	tailored to local contexts and emerging threats.		tion Union (ITU)	12-18 Months for curriculum design and pilot programs.