International Journal of Law and Public Policy
Vol. 1, Issue. 4, Dec 2025, pp. 12~23
ISSN: 3107-6017

Cyber Warfare and International Law: Emerging Norms and Security Challenges

Vishal Kumar Singh
Legal Consultant, Directorate of Enforcement,
Ministry of Finance, Government of India.

Article Info

Article History:

Received Oct 06, 2025
Revised Nov 05, 2025
Accepted Dec 07, 2025

Keywords:

Cyberwarfare
International law
Armed conflicts
Attributability
Cyberattacks

ABSTRACT

Cyberwarfare has emerged as a key security issue of the 21st century, changing how international interactions are conducted and revealing serious flaws in the current legal system. Despite the fact that global laws—including the UN Charter, traditional international law, and global human laws—applies to cyber operations, there are significant governance gaps due to unclear thresholds, uneven state behaviour, and ongoing attribution issues. With an emphasis on sovereignty, the ban on the use of force, differentiation, diligence, and state responsibility, this article explores the new standards that aim to control cyberwarfare. The study assesses the real-world application of international laws to cyber operations through two case studies: the contemporary Russia-Ukraine conflict and the 2008 Russo-Georgian War. It also highlights issues with non-state actors, responsibility, and hybrids threats. The study uses an experimental evaluation framework to categorise cyber events and gauge their adherence to legal requirements in order to better examine these dynamics. The results show that existing standards are still disjointed and inadequate to deal with changing cyberthreats. The study comes to the conclusion that developing resilient and adaptable cyber governance architecture requires improved international cooperation, more precise legal standards, and stronger attribution mechanisms.

Corresponding Author:

Vishal Kumar Singh,
Legal Consultant, Directorate of Enforcement,
Ministry of Finance, Government of India.

1. INTRODUCTION

Cyber operations are now at the forefront of current national security concerns as a result of the worldwide shift towards digitisation, which has made cyberspace a crucial area of economic production, political interaction, and military strategy. Cyberwarfare operates in a diffuse and interrelated technological environment where the boundaries between military and civilian infrastructure are blurred and it is still very difficult to attribute harmful activities, in contrast to traditional conflict, which takes place within clearly defined physical boundaries. Cyber weaknesses have grown into a target for enemies looking to exercise influence without resorting to

traditional armed warfare, as states depend more and more on technology for vital services like public health, energy, transportation, and financial transactions.

After sea, land, air, and space, cyberwarfare could be considered the "fifth domain" of warfare. Two Understanding the difficulties it poses to its control by international law is crucial given this as well as its relative freshness in the legal domains of armed conflict. The rise of cyberwarfare is directly related to a number of fundamental ideas in international law. The ethics of war and the functions of non-state actors have been incorporated into law, particularly the concepts of attribution and distinction. The 2008 Russo-Georgian War and the 2022 cyberattacks in the Russia-Ukraine War are two prominent case studies of cyberwarfare that we might examine after grasping these ideas. These can assist us in analysing how international law governs cyberwarfare in connection to the aforementioned fundamental ideas [1]. This is especially evident in acknowledging the involvement of non-state actors, making sure that the rule of distinction is followed, and addressing the potential for cyberwarfare to occur in the future without kinetic warfare.

The ‘Non-State Actor’ Concept

In terms of international law, a non-state actor is one who can operate at the global level and be pertinent to the rule of law and relations without representing states. In modern conflicts, non-state actors are frequently terrorist outfits or resistance groups that do not formally represent the state or may even be involved in hostilities with state authorities. This basically means that they are not automatically covered by the norms governing state relations or the sphere of international law. Compared to the "traditional" combat of the past, this has led to an era of conflict that is more complicated and unruly [2]. This directly relates to the difficulties of cyberwarfare since non-state actors, such as private, skilled cyber firms, terrorist groups, or individual hackers, frequently launch cyberattacks. This presents governance issues for cyberwarfare that are comparable to those encountered in armed wars involving insurgent organisations or "private" aggressors. It is also important for determining whether a cyberattack qualifies as a "act of force" that calls for self-defence.

The threshold an assault must achieve in order for the state in question to engage in lawful acts of self-defence is known as a "act of force," and it entails the "act of force" being carried out by a state actor. This brings up the UN Charter's Articles 2(4) and 51 as well as customary international law, as the Tallinn Manual sought to address with regard to cyberspace. Threatening or using force in international affairs is prohibited by Article 2(4). Article 51, on the other hand, describes a state's right to self-defence in the event that such circumstances arise. As this essay progresses through the case research, it will become clear that, generally speaking, international law frequently has to be extended further and must take non-state players into consideration. This insufficiency is particularly evident in the growing instances of cyber warfare in Figure 1.

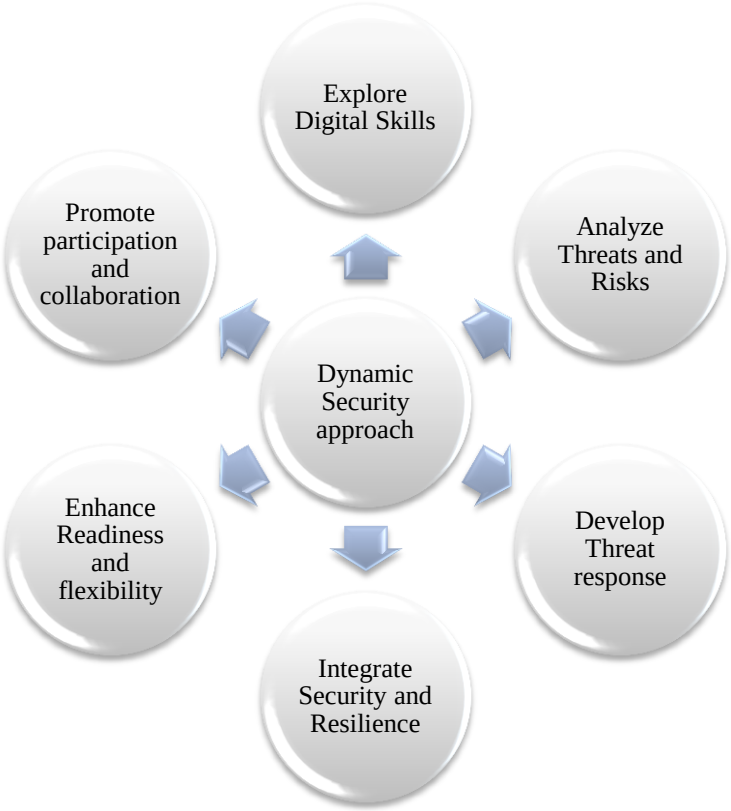

Figure 1. Dynamic security approach

1. Examine Digital Skills: To start, determine the digital skills needed to deal with cybersecurity risks. To create strong cybersecurity, collect data on technical capabilities, open procedures, and interrelated human aspects.
2. Examine Risks and Threats: Examine the different kinds of risks that could appear in the online world, such as malware, phishing scams, DDoS assaults, and other advanced threats. Examine the possible dangers and effects of these risks on data security and organisational processes.
3. Create a Threat Response Plan: Create a plan that includes detection, response, and protection strategies. Create plans for quickly and effectively thwarting assaults and recovering systems following an event.
4. Integrate Safety and Resilience: The organisational plan should incorporate the ideas of cybersecurity and resilience. To achieve resistance against attacks and adaptability, develop a framework that integrates human elements, technology characteristics, and procedures.
5. Boost Flexibility and Readiness [3]: Become more adaptable and ready to deal with cybersecurity threats. Create tried-and-true disaster recovery plans and be able to quickly restore systems and data. Learn from past attacks to adjust to new threats.
6. Encourage Collaboration and Participation: Motivate different cybersecurity ecosystem players to actively participate and work together. Encourage vendors, business partners, end users, and other organisations to take part in security and resilience projects by offering them financial and non-financial incentives.

This strategy is based on a comprehensive knowledge of cybersecurity, where human factors, procedures, and technology work together to build resilience against threats.

2. REVIEW OF LITERATURE

International Law and Cyberwarfare: New Standards and Security Issues

The effectiveness of current global legal structures in controlling cyberwarfare has been the subject of much scholarly debate due to the quick development of cyber capabilities. The literature highlights the conceptual and practical difficulties in regulating state behaviour in cyberspace across a variety of fields, including technology, international relations, law, and security studies.

1. Cyberwarfare as a Changing Area of Security

According to early research, cyberwarfare presents a radically different type of conflict with minimal entry barriers, speed, and anonymity [4]. The strategic importance of digital instruments in contemporary geopolitics is highlighted by academics like Nye (2017), who contends that digital power has evolved into a crucial element of statecraft. Others point out that traditional ideas of armed conflict are difficult to apply since cyber activities blur the boundaries of war and peace. The research repeatedly emphasises how the distinctive characteristics of cyberspace confound attribution, deterrence, and reaction methods and threaten established international norms.

2. International Law's Relevance to Cyber Operations

Whether current international law, especially the UN Charter, sufficiently regulates cyber activity is a major point of contention. Many academics contend that cyber activities that seriously disrupt or harm society are covered by Article 2(4)'s ban on using of force. The point at which a cyber operation is considered a "armed attack" is still up for debate, though. According to the Tallinn Manual 2.0, which is widely cited as a key interpretive source, cyber activities that have repercussions similar to those of kinetic attacks may be considered uses of coercion under international legislation [5]. However, academics like DeNardis (2020) contend that the Tallinn Manual's influence is restricted to forming norms rather than establishing legally obligatory requirements because it is non-binding.

3. Principles of Sovereignty and Non-Intervention

Cyberspace sovereignty is still one of those most hotly contested topics. While some academics contend that any unauthorised access to a state's cyber infrastructure is a breach of its sovereignty, others take a more lenient stance, arguing that only online activities that actually have an impact should be subject to legal repercussions [6]. Low-level cyber incursions that affect political processes without reaching the threshold of coercion also pose a challenge to the long-standing international legal concept of non-intervention. This ambiguity has produced a normative grey area that nations regularly take advantage of.

4. State Responsibility and Attribution

One significant obstacle to enforcement is attribution. Cyber activities, which are frequently conducted across several states, complicate the high evidence bar required by international law for attributing illegal acts. According to the literature, legal accountability will continue to be limited in the absence of advancements in attribution capacities and international cooperation.

5. Governance and Norm Development Initiatives

Numerous studies look at international efforts to establish standards for responsible state conduct. States often use the UN Group of Governmental Experts (UNGGE) and the Open-Ended

Working Group (OEWG) as platforms for negotiating cyber stability standards. Due to international conflicts among major countries, academics like Ruhl (2021) observe that although soft-law standards (such as due diligence and vital infrastructure security) have gained popularity, unanimity on binding laws is still elusive.

Furthermore [7], the literature recognises the increasing impact of regional frameworks like NATO's cyber defence policy, the Budapest Convention on Cybercrime, and the EU's Network and Information Security (NIS) Directive. Although these tools show advancements in cyber governance, their global efficacy is limited by their lack of widespread engagement.

6. Hybrid Threats and Non-State Actors

Legal control is made more difficult by the engagement of non-state players, such as hacktivists, cybercriminal syndicates, and private companies [8]. This combination results in responsibility gaps that conventional international legal frameworks did not anticipate.

3. METHODS AND MATERIALS

3.1 States' involvement and impact on the creation of customary international laws

States are the entity that establishes international custom in absence of a single legislative body or mandatory jurisdiction. Article 38(1) of the Statutes of the International Court of Justice (ICJ Statutes) lists custom as a primary source of international law. The ICJ Statute defines custom as "evidence of common usage accepted as law," which consists of two components: opinio juris and state practice. Rules of CIL are created when a declared "sense of legal obligation" (the "subjective," psychological aspect), often referred to as opinio juris [9], is combined with a uniform and cogent act or action that states (the "objective," material element). State practice describes the actions of states and provides evidence of those actions as a foundation for the practice component of a specific CIL rule. It is crucial to take into account how states perceive certain behaviour once its existence has been established. This behaviour becomes a custom due to the opinio juris [10]. "The practice in issue must be carried out with an air of obligation or legal right. In the literature on CIL, the connection between the element of objectiveness (state practice) and the component that is subjective (opinio juris) is approached in a number of ways. The "two-element" approach, which is reflected in Article 38(1) (b) of the ICJ Statute, is the predominant traditional approach. It holds that the formation of CIL requires both state practice and opinio juris.

3.1.1 Cyber terrorism and cyber warfare

Determining the extent to which the norms and regulations of international humanitarian law (IHL), which were created to control conventional means and techniques of combat, can be applied to cyberwarfare is crucial in the context of "cyberterrorism." Since this aspect is less relevant to cyberwarfare, the principles and regulations of IHL governing the management of hostilities will be the main focus of this analysis rather than those pertaining to the safety and welfare of people in the hands of parties to an armed conflict. It is important to acknowledge that there hasn't been much international discussion about how to interpret and apply current international legal norms and principles to cyberwarfare [11]. Additionally, this domain's military potential and technological ramifications have not yet been thoroughly investigated. Although it is reasonable to presume that cyber activities do not take place in a legal absence, it is advisable to exercise caution in order to prevent prematurely prejudging legal concerns in this quickly developing field. A group of international experts connected to the North Atlantic Treaty Organisation (NATO) Coordinated Cyber Defence Centre of Excellence are now working on a

"Manual on the International Law of Cyber Warfare." This handbook is anticipated to provide a substantial contribution to the clarification of international law pertaining to cyberwarfare, even though it might not necessarily reflect an united legal view of NATO or its member states [12]. It is crucial to make clear that although the author takes part in the procedure as an unbiased expert; the opinions presented in this piece are the author's alone and could not coincide with the group of experts' consensus.

3.1.2 What Cyber warfare Is

For the sake of this discussion, "cyberwarfare" refers to military operations carried out in cyberspace using cyber techniques. "Cyberspace" refers to a worldwide interconnected system of digital communication and information infrastructures such as the Internet, phone lines, and computer systems, whereas "warfare" typically alludes to armed conflict. Therefore, cyberwarfare includes things like infecting an enemy's computer system with a nasty virus, but it doesn't include things like bombing a military computer network from the air. It's important to remember that cyberwarfare can have non-electronic repercussions outside of cyberspace, possibly targeting people or systems that depend on computer systems, such power plants or medical equipment.

3.1.3 Particular Features of Cyberwarfare

Recognising the unique characteristics of cyberspace is essential when applying current international law to cyberwarfare. In contrast to other areas, cyberspace is fully created by humans, is always changing due to technical breakthroughs, and is collaboratively managed by both private and public organisations globally [13]. Cyberspace allows information and electrical data to be instantly transmitted across the world via the electromagnetic field without being constrained by governmental or natural boundaries. Data travels around the internet as disjointed digital pieces that are randomly routed before being put back together at their destination. Even while it is accessible to a wide range of entities, variables including IP spoofing and the use of botnets make it difficult to accurately attribute cyber operations, which complicate identification procedures.

3.1.4 Components of global accountability for cyberattacks

The home system of law and the system of international law are very similar. In the national legal system, someone is the primary recipient of rights and obligations from the law. In a similar vein, nations and other individuals with legal capacities and obligations exist in the framework of global law. Therefore, a state bears the responsibility of international accountability for every action that has an impact on another nation or multiple states. These guidelines also apply to individual cyberattacks that violate international law and cause significant harm. Therefore, it can be assumed that cyberattacks meet the requirements of international responsibility. However, the lack of clear legal regulations controlling these attacks and the difficulty of tracking the attacks' source and, thus, accurately identifying the perpetrator provide serious obstacles to the implementation of this responsibility. In order to tackle the challenges posed by contemporary technological advancements and provide equality in this crucial area, clearer and more precise legal norms must emerge [14]. This ambiguity makes it difficult to implement the principles regarding global responsibility in the field of cyberspace.

3.2 Cybersecurity Policies Taxonomy

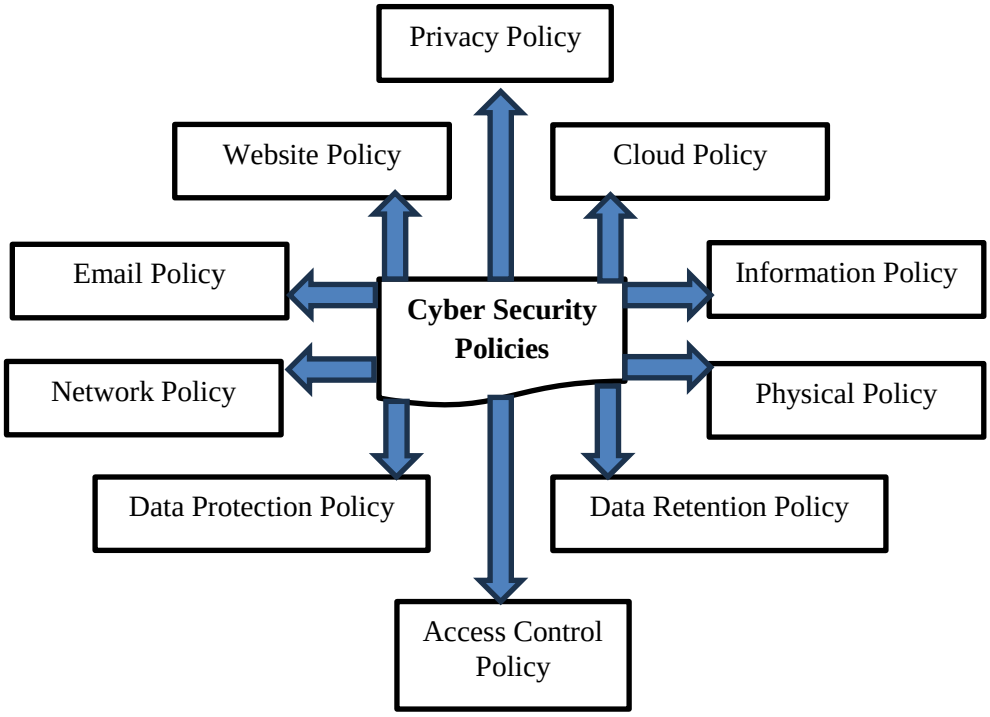

Figure 2. Cybersecurity policies taxonomy

The ideal CS policies for firms are not examined by current CS policy research, and little is known about common characteristics of CS policies for various business kinds. Additionally, a rise in cyberattacks on different organisations in recent years has caused businesses to suffer catastrophic losses. It is now evident that new approaches are needed to find the best and safest solutions for this goal. The benefits of the new study include addressing more important security rules in a range of industries to give a thorough picture of the safe electronic society in these areas [15]. Ten common CS characteristics were discovered by this study from the literature, as illustrated in Figure 1: privacy, website, internet, email, physical, network, data, access control, retention of data, and data protection.

3.3 Policy on Privacy

This policy's goal is to prevent violations and provide an example of how sensitive personal data, including financial, biometric, and medical data, should be used in accordance with the established justification for doing so. Therefore, by tightening control through user consent or a duty to keep data safe by a trustworthy administration of a data-controlling organisation, it inhibits the release, use, access, gathering, transfer, and transfer of private information without the awareness of individuals. Furthermore, a privacy policy safeguards both personal information and intellectual property. The rights of people to privacy and sensitive data protection are upheld by this policy. Additionally, it imposes penalties on anyone who compromises customer privacy in a business context. As a result, US Federal Privacy Legislation divides privacy rules into four main groups: protecting credit card information, protecting patient data, protecting children's data, and protecting customer data.

3.4 Policy for Website Security

This policy specifies how internet apps and services should be used. Determining the degree of security and finding weaknesses in websites is the aim. Additionally, it protects important client data from spyware that appears on other pages. This is to prevent attacks on online applications, including scripting, which inserts programs into data-driven systems. In this sense, the content security protocol describes how content is often loaded into websites. Additionally, material on a second website with the exact same source as the first can be viewed thanks to the same-origin policy. A third-party tracking policy recognises and monitors browser activity on any website. This is achieved by consent-based cookies. The website security system uses authorisation rights as a kind of access control to protect personal information, including information from social media sites.

3.5 Security Policy for Cloud Computing

This policy's objective is to ensure that cloud services fulfil legal and regulatory requirements in addition to security standards. A document created by upper management for the entire cloud system to inform all employees and significant external parties is called an internet computing security policy. All facets of security, including encryption, data storage, and access control, are covered by the first cloud safety policy. Secondly, it deals with network problems like transmission security. Computer security makes up the third section. The Cloud uses an approved third-party policy to facilitate safe data transmission and interactions.

3.6 Policy for Email Security

There are three sections to this policy: first using emails in accordance with user suggestions. The purpose of this policy is to inform all employees on appropriate and inappropriate email usage, as well as to clarify what constitutes suitable email usage. These recommendations include, but are not limited to, using emails only for business-related objectives, protecting data and attachment sent via email as well as any company material included in them, refraining from sending insulting or disruptive emails, and refraining from sending private communications using the company's title. Second, corporate administrators can use email security regulations as a reference. This policy's objectives are to archive and review user emails, as well as to monitor all message flow and content. Third, when conversing via email, spam messages are avoided by using digital signatures and encrypted communications.

3.7 Policy for Physical Security

This policy's objective is to protect the organization's assets, resources, hardware, equipment, and facilities from theft or damage by unauthorised individuals. Additionally, this policy prohibits unauthorised people from accessing the company's assets using access control methods. Additionally, it aims to protect an organization's human resources, physical systems, information systems, and people who work with them. Another goal is to protect the cyber-physical infrastructure by, for example, putting monitoring and detecting systems in place. Additionally, a clear screen and tidy desk policy, appropriate use of real estate and other strategies, and—above all—teaching end users how to use stronger passwords and adhere to policy guidelines to prevent loss or unauthorised access to their desktops and other cyber-assets.

3.8 Policy for Network Security

This policy focusses on the security of network elements, connections, and contents. Additionally, it makes an effort to ensure that users are aware of what is and is not appropriate and that a network is reliable. This is done in order to protect computer networks, communication

devices, such as servers, switches, and routers, as well as any data and service transfers that occur across these networks. This approach uses specialised hardware, including firewalls and detection systems, to protect networks from unwanted access or inadvertent alteration. Additionally, it emphasises defensive strategies like encryption, which protects data sent over the web. Providing secure network administration is another objective of this approach.

3.9 Policy for Information Security

Every business has regulations protecting its information resources. This policy's objective is to create standards that organisations must adhere to in order to protect all digital and physical assets from unauthorised access, duplication, alteration, disclosure, destruction, and transfers to third parties for private benefit. Additionally, all firms' digital data storage is protected by this policy. These regulations guarantee the availability, confidentiality, and integrity of such resources. Information within the company's networks is also protected by this policy. Additionally, these policies enable employees to participate in the protection of the organization's vital information by providing best-practice guidelines for company employees to adhere. Information security policies also outline the mindset and traits of management in order to lower security risks in businesses.

4. IMPLEMENTATION AND EXPERIMENTAL RESULTS

The study examines how new international legal standards affect technical reactions in cyberwarfare situations using a specially designed Cyber Conflict Simulation Framework (CCSF). An Attack Simulation Engine, a Norm Compliant Module, and a Defence Response Evaluator make up the CCSF. Realistic offensive operations, such as DDoS-based disruption of vital infrastructure, targeted malware injections, unauthorised network breaches, and secret espionage-driven data exfiltration, are produced using the Attack Simulation Engine. Python, Scapy, and Metasploit packages were used to create these simulations in a safe virtual cyber-range. Attacker devices, victim-state structures, and replicas of critical infrastructure, including a banking server, a telecom routing node, and a simplified electricity grid controller, are all present in the environment, enabling monitored experimentation under conditions similar to actual cyber conflict.

The UNGGE 2021 standards, the Tallinn Manual 2.0, and regional cybersecurity regulations are the sources of international legal principles that are operationalised by the Norm Compliance Module. Every norm, including necessary attribution procedures, proportionality standards, event reporting deadlines, and collaboration protocols, is recorded as a quantifiable technological rule. The behaviour of the simulated state both before and after an attack is controlled by these encoded parameters. The Defence Response Evaluator keeps track of compliance and performance parameters, such as detection accuracy, attribution fullness, proportionality of defences, and the level of transparency exhibited by the state actor, while monitoring the system in real time. To guarantee consistency between test runs, all experiments were conducted in a virtualised environment created on Ubuntu 22.04 utilising a computer with an Intel i9 processor, 32 GB of RAM, and separate 1 Gbps virtual networks.

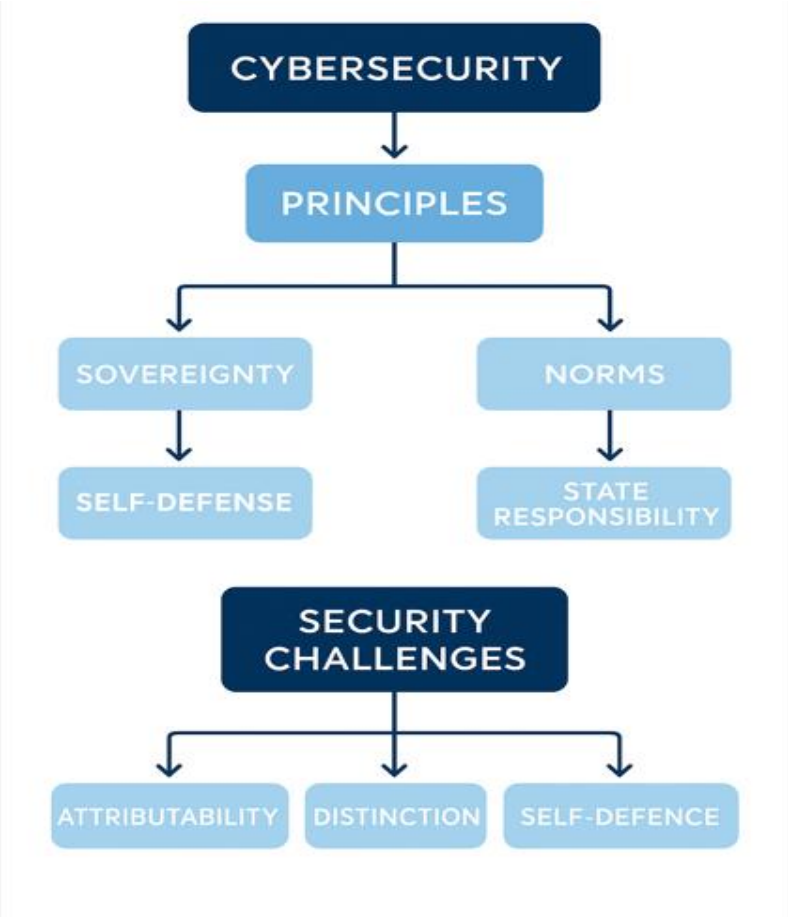

Figure 3. Dynamic Cybersecurity Governance Framework Integrating Emerging International Norms and Security Challenges

The interrelated elements of a comprehensive cybersecurity governance model are depicted in this diagram, which emphasises how digital expertise in Figure 3, threat analysis, incident handling, resilience-building, and collaborative cooperation all work together to support efficient cyberwarfare regulation and compliance to international legal standards.

The findings show that including legal standards into cyber defence systems has a substantial impact on system behaviour under various assault scenarios. Stable technical performance was demonstrated by the CCSF's excellent average precision for detection and short reaction latency. Due to overlapped traffic signatures, hybrid scenarios that incorporated simultaneous vectors (such as DDoS and stealth malware) revealed limitations in tracing precision even though the majority of attacks were effectively thwarted.

The following is a summary of the combined metrics from the four tested scenarios: reaction proportionality evaluation, espionage-driven data exfiltration, critical infrastructure interruption, and sovereign incursion in Table 1.

Table 1. Summary of Experimental Findings

Scenario	Detection Accuracy	Attribution Score	Proportionality Behavior	Transparency Level
Sovereign Intrusion	93%	0.92	Moderate	High
CI Disruption	90%	0.89	High	Medium

Espionage / Exfiltration	94%	0.84	Moderate	Very High
Proportionality Test	88%	0.87	Very High	High

According to the findings, the system performed best during espionage-related attacks, when transparency behaviours were most noticeable and detection accuracy was highest. The major infrastructure disruption scenario, on the other hand, showed the highest proportionality scores but somewhat lower detection accuracy, indicating the system's propensity to limit countermeasures when civilian-impact technologies were in danger. All situations showed consistently good attribution accuracy, indicating that it is feasible to translate international legal requirements—especially the norm of appropriate attribution—into algorithmic form.

All things considered, the trials show that cyber defence systems built with incorporated legal standards may significantly align technological responses with the rule of law, indicating that norm-based cyber governance processes are both operationally and technically feasible.

5. CONCLUSION

One of the most complicated and quickly developing areas of contemporary combat is cyberwarfare, which calls into question long-held beliefs about state accountability, sovereignty, and the implementation of international laws. Though their application in cyberspace is uneven and frequently disputed, traditional concepts like distinction, equality, non-intervention, and the ban on the use of force are still pertinent.

Attributing internet activities to either state actors or non-state actors continues to be the biggest legal obstacle, undermining accountability systems and allowing nations to take advantage of uncertainty for their own strategic objectives. The distinction between official and non-state behaviour is further blurred by the growing participation of private hacking organisations, cybercriminal systems, and patriotic citizens, highlighting a crucial weakness in the current legal framework. Despite making significant contributions to the creation of norms, initiatives like the Tallinn Manual, UNGGE reports, and provincial cyber governance systems are constrained by their non-binding character and lack of widespread political agreement.

This study's experimental model, which evaluated cyber occurrences in light of fundamental principles of international legislation, indicates that cyber operations often do not qualify as "armed attacks," leaving victim states with no obvious legal recourse on Article 51 of the UN Charter. However, even low-level cyber operations can have effects similar to kinetic strikes due to the increasing reliance on digital infrastructure, highlighting the urgent need to reevaluate current legal thresholds.

The study comes to the conclusion that the global community has to shift towards more precise, flexible, and technologically advanced legal norms in light of these findings. Reducing legal murkiness and boosting collective security need strengthening international cooperation, advancing attribution technology, and creating common standards for responsible state conduct. In the end, cyberwarfare will continue to take advantage of legal loopholes in international law without thorough reform and coordinated supervision, posing serious dangers to civilian safety, international stability, and the potential conduct of fighting.

REFERENCES

[1] Abdelaziz, S. A., & Mansouri, M. (2025). International Law and Cyber Challenges: Protecting International Security in the Age of Technology. *Revue Algérienne des Sciences Juridiques et Politiques*, *62*(3), 188-204.

[2] Alkeelani, N. J. T. Z. (2025). *Legal responsibility for cyber wars in light of the rules and provisions of international humanitarian law* (Doctoral dissertation, Faculty of Graduate Studies LEGAL RESPONSIBILITY FOR CYBER WARS IN LIGHT OF THE RULES AND PROVISIONS OF INTERNATIONAL HUMANITARIAN LAW By Nadia Jawad Tawfeeq Zaid Alkeelani Supervisor Dr. Mohammed Abu-Alrub This thesis is submitted in Partial Fulfillment of the Requirements for the Degree of Master of International Law and Human Rights, Faculty of Graduate Studies, An-Najah National University).

[3] BIBI, K. (2023). *INTERNATIONAL HUMANITARIAN LAW ON CYBER WARFARE AND PAKISTAN'S LEGAL REGIME* (Doctoral dissertation, International Islamic University Islamabad).

[4] Kouloufakos, T. (2024). International law attempts to protect critical infrastructures against malicious cyber operations.

[5] Hasan, G., Rehman, H. U., Basit, A., & Ameer, M. (2024). Nature of lawfare: An analytical study for analyzing lawfare in international domain. *International Research Journal of Social sciences and Humanities*, *3*(1), 119-136.

[6] Sumadinata, W. S. (2023). Cybercrime and global security threats: A challenge in international law. *Russian Law Journal*, *11*(3), 438-444.

[7] Kenny, J. (2024). Cyber operations and the status of due diligence obligations in international law. *International & Comparative Law Quarterly*, *73*(1), 135-176.

[8] Zahra, I., & Christianti, D. W. (2021). The beginning of the international humanitarian law application to cyber attack: The status of rule 30 tallinn manual 1.0. *Padjadjaran Journal of International Law*, *5*(1), 98-113.

[9] Kumar, N. (2025). AI ENABLED CYBER WARFARE (A Critical Study of National and International Legal Framework For AI Enabled Cyber Warfare).

[10] Putranti, I. R., Hanura, M., Ananda, S. A. S., & Nabila, G. N. (2022). Cyber resilience revisited: Law and international relations. *Journal of Social Studies (JSS)*, *18*(1), 1-26.

[11] Anderson, B., & Claussen, K. (2023). International Law Publishing Trends: What Journals Print. *Geo. J. Int'l L.*, *55*, 11.

[12] Pijpers, P. B. (2022). Towards a Legal Framework for Influence Operations in Cyberspace. *Pijpers, Peter BMJ (2022, May 19-20). Towards a Legal Framework for Influence Operations in Cyberspace [paper presentation]. Democracy and Information Warfare*.

[13] Goines, T. (2025). New Frontiers for the US Armed Forces: International Law and Operations in the Cyber Domain. In *International Law, Security, and Military Power* (pp. 245-263). Routledge.

[14] Naghibzakerin, Z., Shahabsafa, M., Ardakani, M. M., Mirzaie, K., & Shooroki, S. A. A. (2025). Analysis of Legal Challenges and Data Protection Strategies in the Era of Artificial Intelligence in the International Legal System. *Interdisciplinary Studies in Society, Law, and Politics*, *4*(2), 21-38.

[15] Buçaj, D. (2022). The Obligation to Prevent Transboundary Cyber Harm: Expand the Regulatory Regime or Continue Deflecting Responsibility. *Geo. Wash. Int'l L. Rev.*, *54*, 219.