WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cyber Welfare and State Responsibility under Public International Law: Emerging Challenges and Legal Responses

Mohamed Ashif M[1], S. Ragupathi[2]

[1] 1st Year Llb(Hons), Chettinad Academy Of Research And Education, Kelambakkam 600103, India,
[2]Assistant Professor, Chettinaf Academy Of Research And Education, Kelambakkam 603103, Tamilnadu, India.

ABSTRACT

In the contemporary era, cyber warfare has emerged as a pivotal aspect of international security, challenging traditional conceptions of armed conflict and state responsibility under public international law. Unlike conventional warfare, cyber operations are characterized by anonymity, cross-border reach, rapid execution, and non-physical yet potentially catastrophic impacts on critical infrastructure, economy, and national security. This creates significant legal and practical difficulties in attribution, accountability, and enforcement, raising questions about the applicability of existing international legal frameworks. This paper examines the emerging challenges posed by cyber operations, focusing on the principles of state responsibility, including direct involvement, effective control, and complicity of non-state actors. It analyzes whether cyber-attacks constitute a "use of force" under Article 2(4) of the UN Charter, how violations of state sovereignty are assessed, and the extent to which states can be held liable for actions carried out through intermediaries. The study critically evaluates the contributions of non-binding instruments, such as the Tallinn Manual 2.0, and considers UN resolutions and customary international law as frameworks for regulating cyber conduct.The paper argues that while current legal principles provide a foundation for state accountability, they are often inadequate for addressing the speed, scale, and complexity of cyber operations.

KEYWORDS: Cyber warfare, State responsibility, Public international law, Tallinn Manual, Attribution, Use of force, Sovereignty, International humanitarian law, Emerging legal challenges, Cyber operations.

INTRODUCTION

The rapid advancement of digital technologies has fundamentally transformed the nature of international conflict and security, giving rise to cyber warfare as a critical component of modern statecraft. Cyber operations—ranging from espionage, sabotage, and disruption of critical infrastructure to offensive military campaigns—have introduced a complex set of challenges for public international law. Unlike conventional kinetic warfare, cyber attacks can be executed remotely, anonymously, and across borders, often without immediate physical destruction but with significant economic, social, or political consequences. These unique characteristics complicate traditional legal concepts such as sovereignty, the use of force, and state responsibility, raising pressing questions about the applicability and adequacy of existing legal frameworks.[1]

Cyber warfare is distinguished by its speed, scope, and invisibility. States may deploy malware, ransomware, or denial-of-service attacks to disrupt essential services, manipulate information systems, or target military and civilian infrastructure [2].The anonymity inherent in cyberspace makes attribution—identifying the responsible actor—particularly difficult. Moreover, many cyber operations are conducted by non-state actors, including criminal organizations, hacktivist groups, or proxy entities, sometimes with state sponsorship or tacit support. Under international law, the responsibility of states for cyber operations conducted by such actors hinges on principles of effective control, direction, or complicity, which are still evolving in both legal scholarship and practice.[3]

Under the United Nations Charter, states are prohibited from the threat or use of force against the territorial integrity or political independence of another state (Article 2(4)), and they have the right to self-defense against armed attacks (Article 51). [4]The challenge lies in determining whether a cyber operation constitutes a "use of force" or an "armed attack" comparable to traditional military action. Cyber attacks may cause disruption to power grids, transportation systems, financial institutions, or communication networks, potentially resulting in economic damage or loss of life indirectly. While some legal scholars argue that only physical damage qualifies as a use of force, others contend that cyber operations with equivalent strategic effects should be

[1] Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2017), 45.
[2] Joseph S. Nye, Cyber Power (Cambridge, MA: Harvard University Press, 2010), 22.
[3] Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2017), 89–91.
[4] United Nations, Charter of the United Nations, 26 June 1945, 1 UNTS XVI, Articles 2(4) and 51.

treated similarly under international law. This debate illustrates the need to reinterpret and adapt traditional legal norms to address emerging digital threats[5].Another critical dimension is the principle of state sovereignty. In the physical world, sovereignty is linked to territorial integrity and exclusive control over national territory. In cyberspace, sovereignty extends to the protection of a state's critical networks and infrastructure. Unauthorized intrusion, data manipulation, or sabotage conducted remotely from outside a state's borders constitutes a violation of sovereignty, raising complex legal questions about jurisdiction, permissible countermeasures, and remedies. Determining the threshold at which a cyber intrusion breaches sovereignty or triggers the right of self-defense is one of the most significant challenges in contemporary international law.

The evolving nature of cyber threats has prompted the development of normative frameworks to guide state behavior. Notable among these is the Tallinn Manual 2.0, which offers detailed analysis on the applicability of international law to cyber operations, including rules governing attribution, state responsibility, and the use of force. Although non-binding, the manual provides a widely recognized reference for policymakers, legal scholars, and military strategists. Similarly, resolutions by the United Nations Group of Governmental Experts (GGE) have emphasized that international law, including the prohibition of aggression, sovereignty, and human rights obligations, applies in cyberspace, reinforcing the principle that cyber operations are not outside legal scrutiny.[6]

Despite these developments, significant gaps remain. Current international law was primarily designed for kinetic armed conflict and does not adequately address the complexity, transnational nature, or speed of cyber operations. Attribution remains technically and legally challenging, particularly when non-state actors operate with varying degrees of state support. Existing treaties and conventions provide limited guidance on proportionality, acceptable targets, or the rights and obligations of states in cyberspace. The lack of binding international agreements specific to cyber warfare leaves states navigating a largely uncertain legal landscape, increasing the risk of disputes and escalation.[7]

Given these challenges, the question of state responsibility in cyber warfare has become central. States must be held accountable for cyber operations that violate international law, whether directly executed or indirectly enabled. Establishing clear principles of responsibility, attribution, and legal thresholds for intervention is essential to ensure accountability, deterrence, and stability in the digital domain. At the same time, states must balance national security interests with legal compliance, fostering norms of responsible behavior without undermining legitimate cyber defense capabilities.[8]

This paper aims to examine the emerging challenges of cyber warfare, focusing on the principles of state responsibility under public international law. It explores how traditional legal concepts, such as sovereignty, use of force, and accountability, are being interpreted in the cyber context, and evaluates the legal responses developed through instruments like the Tallinn Manual, UN resolutions, and customary international law. By analyzing these frameworks, the study seeks to identify gaps, challenges, and potential solutions for governing state conduct in cyberspace, emphasizing the need for cooperative, normative, and legally grounded approaches to address one of the most pressing security challenges of the 21st century.[9]

C. RESEARCH OBJECTIVES

1. To examine the concept of cyber warfare and its evolution in the context of modern international security, highlighting the key technological, strategic, and operational characteristics that differentiate it from conventional armed conflict.

2. To analyze the principles of state responsibility under public international law in relation to cyber operations, including attribution, effective control, and accountability for actions carried out directly or through non-state actors.

3. To evaluate the applicability of existing international legal frameworks, including the UN Charter, international humanitarian law, and customary international law, in regulating state conduct and cyber operations.

4. To identify emerging challenges and legal gaps in addressing cyber warfare, such as difficulties in attribution, defining use of force, protecting sovereignty, and regulating actions by non-state actors.

5. To assess current and potential legal responses, including the Tallinn Manual, UN resolutions, and proposed multilateral agreements, and to recommend strategies for improving accountability, cooperation, and compliance in cyberspace.

[5] Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2017), 101–103.
[6] Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2017), 7; United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 (2015), 4–5.
[7] Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2017), 112–115; Joseph S. Nye, Cyber Power (Cambridge, MA: Harvard University Press, 2010), 28–30.

[8] Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2017), 130–133; Matthew C. Waxman, "Cybersecurity and International Law," Yale Journal of International Law 40, no. 2 (2015): 321–322.
[9] Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2017), 5–7; Joseph S. Nye, Cyber Power (Cambridge, MA: Harvard University Press, 2010), 18–20.

D.RESEARCH QUESTIONS

1. What constitutes cyber warfare under public international law, and how does it differ from conventional armed conflict?

2. How is state responsibility determined in cyber operations, especially when non-state actors or proxies are involved?

3. To what extent do existing international legal frameworks, including the UN Charter, customary international law, and international humanitarian law, regulate cyber warfare?

4. What are the key challenges in attributing cyber attacks, defining the use of force, and ensuring accountability for violations of sovereignty in cyberspace?

5. What legal responses and normative frameworks, such as the Tallinn Manual and UN resolutions, exist to address state responsibility in cyber warfare, and how effective are they?

E.RESEARCH HYPOTHESES

The research hypotheses for this study are designed to explore the complex interplay between cyber warfare and state responsibility under public international law. The first hypothesis (H1) posits that cyber operations present unique challenges that existing international legal frameworks, such as the UN Charter, customary international law, and international humanitarian law, are insufficient to address comprehensively due to the rapid technological evolution.

anonymity of actors, and transnational nature of attacks. The second hypothesis (H2) focuses on state accountability, suggesting that states can be held responsible for cyber operations conducted by non-state actors or proxies if there is evidence of effective control, direction, or support, aligning with principles established in traditional international law on state responsibility. The third hypothesis (H3) emphasizes that the lack of clear attribution mechanisms significantly undermines enforcement and limits the ability of states to hold perpetrators accountable. The fourth hypothesis (H4) contends that non-binding instruments, such as the Tallinn Manual 2.0, provide valuable guidance but are inadequate in the absence of binding treaties or multilateral agreements. Finally, H5 asserts that the development of multilateral cooperation, legal norms, and technical attribution frameworks will enhance compliance, deter cyber attacks, and strengthen accountability in cyberspace. Collectively, these hypotheses guide the study toward evaluating both legal and practical dimensions of cyber warfare.

F.STATEMENT OF THE PROBLEM

The emergence of cyber warfare as a tool of statecraft has created a complex set of challenges for public international law, exposing gaps in traditional legal frameworks designed for conventional armed conflict. Cyber operations—ranging from espionage, sabotage, and disruption of critical infrastructure to offensive digital attacks—often occur across borders, with anonymity, and through non-state actors, complicating the application of legal principles such as sovereignty, use of force, and state responsibility. Attribution of cyber attacks remains particularly difficult, as it requires establishing a clear link between the action and a state, especially when proxies or criminal networks are involved. Existing legal instruments, including the UN Charter, customary international law, and the Geneva Conventions, were drafted in the context of kinetic warfare and do not adequately address the speed, scale, and non-physical impacts of cyber operations. Non-binding guidance like the Tallinn Manual 2.0 offers interpretative assistance but lacks enforceability. This legal uncertainty poses risks of unregulated state behavior, escalation of conflicts, and lack of accountability, potentially undermining international peace and security. Therefore, the core problem addressed by this study is the inadequacy of current international legal frameworks to regulate, attribute, and ensure accountability for cyber operations, highlighting the urgent need for clarity, normative development, and cooperative mechanisms to govern cyber warfare effectively.

G.LITERATURE REVIEW

1. Attribution in Cyber Warfare

Attribution is the process of identifying the actor responsible for a cyber operation, which is critical for establishing state responsibility. Tsagourias and Farrell (2020) highlight that attribution is both a technical and legal challenge. Even when forensic techniques can trace attacks, linking them conclusively to a state actor is difficult, especially when proxies or criminal groups are involved. This complicates enforcement of international law, as legal thresholds for state responsibility require clear proof of control or direction.

Website: Oxford Academic – European Journal of International Law

2. Applicability of International Law to Cyber Operations

Jiang (2019) discusses the challenges of applying existing international law to cyber warfare. While the UN Charter, customary international law, and IHL formally apply, they were originally designed for conventional armed conflict and struggle to address non-physical and transboundary cyber attacks. Jiang suggests establishing an independent fact-finding mechanism to address evidentiary and attribution difficulties in cyber operations.

Website: LSE Law Review

3. Cyber Operations Against Critical Infrastructure

Manahan (2021) examines how cyber attacks on critical infrastructure interact with international norms. The UN has proposed a norm prohibiting attacks on another state's essential infrastructure. However, questions remain about the definition of critical infrastructure, threshold for damage, and the relationship to the use of force principle. This ambiguity complicates legal assessments and state accountability.

Website: Oxford Academic – International Journal of Law and Information Technology

4. State Responsibility and Wrongful Cyber Acts

Delerue (2018) analyses state responsibility under the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA) in the context of cyber operations. The study argues that while the ARSIWA framework is applicable, cyber operations' unique features—such as anonymity and lack of physical damage—complicate attribution, liability, and remedies. This highlights the need to adapt classical principles of state responsibility to the digital age.

Website: Cambridge University Press

5. State Practice and Policy Responses

The Chatham House report (2019) examines how states currently interpret international law regarding cyberattacks. While there is consensus that international law applies, state practice is inconsistent, particularly on issues like sovereignty and use of force. This

inconsistency contributes to legal uncertainty, and the study recommends clearer statements from states on their interpretation of legal obligations in cyberspace.

Website: Chatham House

H. CHAPTERISATION

The research paper is structured into eight comprehensive chapters to ensure a systematic and coherent presentation of the study. Chapter 1 (introduction)provides the background of the study, the statement of the problem, research objectives, questions, hypotheses, significance, and scope, establishing the foundation of the research. Chapter 2(emerging challenges and legal perspective in cyber warfare) critically examines existing scholarly work, legal frameworks, and policy analyses on cyber warfare, attribution, state responsibility, and international law, highlighting gaps that justify the study. Chapter 3) emerging challenges and legal perspective in cyber warfare)explains the research design, data sources, collection methods, and analytical techniques employed to investigate the legal and practical dimensions of cyber operations. Chapter 4(attribution,sovereignty ,and accountability in cyberspace)presents relevant cyber incidents such as stuxnet and notpetya, analyzing state involvement and associated legal challenges. Chapter 5(findings and suggesstion)summarizes findings, addresses research questions and hypotheses, and outlines the study's contribution to knowledge. This chapterisation ensures clarity, logical flow, and comprehensive coverage of the research topic.

CHAPTER 1: INTRODUCTION

The rapid advancement of digital technologies has fundamentally transformed the conduct of international relations and the nature of conflicts. In the modern era, cyber warfare has emerged as a critical component of state power, enabling countries to pursue strategic objectives without traditional kinetic warfare. Cyber operations can range from espionage, sabotage, and disruption of critical infrastructure to full-scale offensive digital attacks. Unlike conventional military operations, cyber attacks are often anonymous, transboundary, and instantaneous, making them difficult to detect, attribute, and regulate.

Under public international law, states are bound by principles such as sovereignty, non-intervention, prohibition of the use of force (Article 2(4) of the UN Charter), and state responsibility for internationally wrongful acts. However, the unique characteristics of cyber operations present significant legal and practical challenges. Questions such as when a cyber operation constitutes a "use of force," how to attribute cyber attacks to states or non-state actors, and what measures are lawful in response remain unresolved. This legal uncertainty is compounded by the rapid evolution of technology and the lack of binding international treaties specifically governing cyber warfare.

CHAPTER 2 : EMERGING CHALLENGES AND LEGAL PERSPECTIVE IN CYBER WARFARE

Cyber warfare has become one of the most pressing challenges in contemporary international relations, presenting complex legal, ethical, and security issues. Unlike conventional armed conflicts, cyber operations are often anonymous, transboundary, and instantaneous, making

detection, attribution, and regulation extremely difficult. Scholars and legal experts recognize that traditional frameworks of public international law—such as the UN Charter, customary law, and International Humanitarian Law—were designed for kinetic warfare and are often insufficient to address the unique nature of cyber operations. Attribution remains a central challenge, as it requires not only technical forensic analysis but also careful legal interpretation to determine whether a state can be held responsible for actions conducted directly or through proxies. Without reliable attribution, enforcing

principles of state responsibility under the Articles on Responsibility of States for Internationally Wrongful Acts becomes highly challenging.In addition to attribution, applying existing international law to cyberspace presents difficulties because concepts such as use of force and sovereignty are difficult to interpret in virtual contexts. While these laws formally apply, practical implementation remains ambiguous, leaving states without clear guidance on lawful conduct or accountability. Scholars suggest that developing binding international treaties or cyber-specific legal instruments could address these gaps and provide clearer normative frameworks.Cyber attacks on critical infrastructure, such as power grids, financial networks, and transportation systems, further complicate legal analysis. Although UN norms discourage attacks on another state's essential infrastructure, ambiguity persists regarding what qualifies as critical infrastructure, the threshold of damage, and how such attacks relate to the use of force. This uncertainty makes it difficult to hold states accountable and highlights the need for more precise international norms and enforcement mechanisms.

Additionally, cyber operations' deniability, lack of physical damage, and cross-border routing complicate legal enforcement. Even when attribution is possible, establishing remedies and reparations remains difficult. Scholars emphasize the need for adapting existing legal frameworks, combining technological, policy, and legal approaches to ensure effective accountability for state-sponsored cyber operations.

CHAPTER 3 : APPROACH TO STUDYING LEGAL CHALLENGES IN CYBERSPACE

This study employs a descriptive-analytical research approach to explore the complex interplay between cyber warfare and state responsibility under public international law. The descriptive component facilitates a comprehensive review of existing scholarly works, legal frameworks, international treaties, and policy documents, while the analytical aspect focuses on interpreting these sources to identify challenges, gaps, and emerging trends. The study relies primarily on secondary data, including academic books, journal articles, international legal instruments, official reports, and case analyses, providing both theoretical insights and practical perspectives on cyber operations.A case study approach is incorporated to examine notable cyber incidents, such as Stuxnet, NotPetya, and other state-attributed attacks. These case studies are analyzed to understand how states are implicated, the application of international law, and the limitations of current accountability mechanisms. This methodology allows for a qualitative analysis of legal principles, state behavior, and scholarly debates to draw meaningful conclusions about cyber responsibility and compliance.The research emphasizes validity and reliability, ensuring that all sources are credible, relevant, and academically rigorous. Primary legal documents and peer-reviewed scholarly works are prioritized to maintain objectivity and accuracy. Ethical considerations are also observed, with sensitive or classified information handled responsibly, ensuring the study adheres to academic integrity standards.

CHAPTER 4 : ATTRIBUTION,SOVEREIGNTY ,AND ACCOUNTABILITY IN CYBERSPACE

Cyber warfare presents unique challenges to traditional concepts of attribution, sovereignty, and accountability under public international law. Attribution—the process of determining the actor responsible for a cyber operation—is one of the most significant hurdles in cyberspace. Unlike conventional military attacks, cyber operations can be conducted anonymously, routed through multiple countries, and executed via non-state actors, making it difficult to definitively identify the perpetrator. Legal frameworks, such as the Articles on Responsibility of States for Internationally Wrongful Acts, require clear evidence that a state directed, controlled, or endorsed a cyber attack to establish responsibility. Without reliable attribution, enforcing accountability becomes nearly impossible, and states may exploit this ambiguity to engage in hostile actions without facing legal consequences.The principle of sovereignty is similarly complicated in cyberspace. International law recognizes the sovereignty of states over their territory and internal affairs, but cyber operations often cross borders without physical intrusion. This raises questions about what constitutes a violation of sovereignty in the digital realm. For instance, if a cyber operation disrupts critical infrastructure or governmental systems remotely, it may infringe upon a state's sovereignty, but the absence of physical presence creates legal ambiguity. Scholars argue that establishing clear thresholds for sovereignty violations is crucial to prevent escalation and maintain stability in international relations.Accountability in cyberspace extends beyond attribution and sovereignty. Even when a cyber operation is attributed to a state, holding it accountable requires mechanisms for legal redress, sanctions, or reparations. Current international law lacks binding instruments specifically designed for cyberspace, and most responses rely on diplomatic, economic, or political measures rather than enforceable legal remedies. Non-binding frameworks, such as the Tallinn Manual, provide guidance but cannot compel compliance. Therefore, ensuring accountability in cyberspace requires a combination of technological attribution, legal clarity, multilateral cooperation, and normative development, enabling the international community to respond effectively to cyber threats while upholding the rule of law.

The study reveals several critical findings regarding cyber warfare and state responsibility under public international law. First, attribution remains the most significant challenge, as cyber operations can be conducted anonymously or through non-state actors, making it difficult to establish legal responsibility. Second, the principle of sovereignty in cyberspace is ambiguously defined, particularly regarding cross-border cyber operations that disrupt critical infrastructure without physical intrusion. Third, current international legal frameworks, while theoretically applicable, are insufficiently adapted to cyberspace, creating gaps in enforcement, accountability, and deterrence. Fourth, state practices are inconsistent: some states follow established norms of responsible behavior, while others exploit legal ambiguities to conduct hostile cyber operations without facing consequences. Finally, non-binding instruments like the Tallinn Manual provide guidance but lack enforceability, limiting their practical impact in ensuring accountability and compliance.Based on these findings, several suggestions emerge to strengthen international legal and policy responses. First, enhancing technical and legal attribution mechanisms is essential to reliably identify perpetrators and hold states accountable. This could involve developing international forensic standards and shared intelligence frameworks. Second, there is a need to clarify the application of sovereignty in cyberspace, defining thresholds for violations and establishing legal consequences for unauthorized interference in critical infrastructure. Third, the international community should pursue

binding treaties or multilateral agreements specifically addressing cyber operations, ensuring clear norms for state behavior, accountability, and reparations. Fourth, capacity-building and cooperation among states should be prioritized, including information-sharing, joint response mechanisms, and diplomatic engagement to reduce risks of escalation. Finally, combining legal, technical, and policy approaches can create a comprehensive framework for cyber governance, ensuring that states act responsibly while protecting international peace and security.

I.CONCLUSION

The rapid advancement of technology has transformed the nature of conflict, bringing cyber warfare to the forefront of international security concerns. Unlike conventional military operations, cyber attacks are often covert, transboundary, and non-physical, making detection, attribution, and accountability uniquely challenging. This research demonstrates that while traditional principles of public international law—such as sovereignty, prohibition of the use of force, and state responsibility—remain applicable, their practical enforcement in cyberspace is limited. The involvement of non-state actors, the use of anonymized networks, and the global reach of cyber operations create legal ambiguities that challenge existing frameworks. Furthermore, inconsistencies in state practice, combined with the non-binding nature of instruments like the Tallinn Manual, highlight the gap between legal theory and practical enforcement.The study also emphasizes that attribution is the cornerstone of accountability. Without reliable attribution mechanisms, states may conduct cyber operations with impunity, undermining international peace and security. Similarly, the concept of sovereignty in cyberspace is not clearly defined in existing law, creating confusion regarding what constitutes a violation when critical infrastructure or governmental systems are targeted remotely. These challenges underscore the pressing need for clarification, codification, and harmonization of legal norms in the digital domain.To address these challenges, a multi-pronged approach is essential. Strengthening technical and legal mechanisms for attribution, developing binding international treaties, fostering multilateral cooperation, and standardizing state practices can collectively enhance accountability. Moreover, integrating legal frameworks with technological tools and policy mechanisms will ensure that states adhere to their international obligations while minimizing risks of escalation. By adopting such comprehensive measures, the international community can reinforce the principle that states remain responsible for their cyber operations, whether conducted directly or through proxies.In conclusion, cyber warfare presents unprecedented challenges, but it also offers an opportunity to adapt and modernize international law. By bridging the gap between legal norms, technological realities, and policy responses, states and international institutions can establish a robust framework for regulating cyber operations, protecting critical infrastructure, and upholding accountability. Ensuring that the principles of international law remain relevant in the digital era is not only a legal necessity but also a critical step toward maintaining global peace, security, and trust in cyberspace.