E-JUSTICE: JOURNAL OF LAW AND TECHNOLOGY

Vol. 1 No. 2, Jan-Jun 2025, pp 46-62

Research Article

State-Sponsored Cyberattacks: Bridging the Gaps in International Criminal Accountability

Andi Agus *Salim*[1]

Corresponding e-mail: andiagus@unja.ac.id

Article Information

Article history
Received: Dec 31, 2024
Revised: Jul 30, 2025
Accepted: Jul 31, 2025

Keywords:
Cyberattacks; Digital Age; Cyberspace; Cyber Warfare; Cybercrime

How to Cite:
Salim, Andi Agus. "State-Sponsored Cyberattacks: Bridging the Gaps in International Criminal Accountability." E-Justice: Journal of Law and Technology 1, no. 2 (2025): 46-62

Abstract

Background: *State-sponsored cyberattacks have become a significant global threat, undermining national security, critical infrastructure, and international relations. These attacks are often difficult to attribute due to the use of proxy actors and the anonymity afforded by cyberspace. Existing international legal frameworks struggle to address the complexities of cyber warfare and hold states accountable for such actions.*

Methodology: *This research employs a qualitative approach, analyzing key case studies of state-sponsored cyberattacks (e.g., Stuxnet, SolarWinds) and reviewing relevant international treaties such as the Budapest Convention and the Tallinn Manual. The study also explores customary international law and state responsibility in the cyber context, with an emphasis on the gaps and challenges in the current legal system.*

Objectives: *The primary aim of this research is to identify the deficiencies in international legal frameworks that hinder the prosecution of state-sponsored cyberattacks. The study proposes legal and institutional reforms to bridge these gaps and enhance mechanisms for attribution and accountability in cyberspace.*

[1] Faculty of Law, Universitas Jambi, Indonesia | https://orcid.org/0000-0001-5638-817X

Findings: *The research highlights the need for robust international frameworks to address state-sponsored cyberattacks. Expanding ICC jurisdiction, new treaties, and forensic advancements are essential. Balancing sovereignty, addressing geopolitical resistance, and learning from past cases are crucial for creating effective, collaborative solutions to cyber threats.*

Originality/Novelty: *This study offers a comprehensive analysis of the intersection between international criminal law and cyber operations, proposing reforms to strengthen accountability mechanisms for state-sponsored cyberattacks. It contributes to the academic discourse by addressing legal gaps and proposing solutions for the evolving digital threat landscape.*

Introduction

In the digital age, cyberattacks have emerged as one of the most significant threats to global security, disrupting economies, compromising critical infrastructure, and undermining political stability. Unlike traditional forms of warfare, cyberattacks operate within the intangible sphere of cyberspace, where borders are blurred, and perpetrators can act with relative anonymity. Increasingly, states are leveraging this domain to achieve strategic objectives, engaging in state-sponsored cyberattacks that target other nations' sovereignty and security.[1]

State-sponsored cyberattacks refer to malicious activities in cyberspace carried out directly by, or with the support of, a state actor. These attacks often aim to compromise the critical infrastructure of adversaries, disrupt political systems, or gain access to sensitive data. Notable examples include the Stuxnet worm, allegedly deployed to sabotage Iran's nuclear program; the 2016 U.S. election interference attributed to Russian operatives; and the SolarWinds hack, which infiltrated numerous government and private sector networks

[1] Henry Durojaye and Oluwaukola Raji, "Impact of State and State Sponsored Actors on the Cyber Environment and the Future of Critical Infrastructure," version 1, preprint, arXiv, 2022, https://doi.org/10.48550/ARXIV.2212.08036.

worldwide. These incidents highlight the growing sophistication and impact of state-backed operations, which blur the lines between acts of war, espionage, and criminality.[2]

The increasing prevalence of state-sponsored cyberattacks has exposed significant gaps in international law. Traditional frameworks of international law were developed to address physical acts of aggression and criminality; they often fail to account for the unique characteristics of cyber operations. The anonymity of cyberspace, the use of proxy actors, and the difficulty of attributing actions to a specific state all complicate efforts to hold perpetrators accountable. Moreover, existing treaties, such as the Budapest Convention on Cybercrime, are not adequately equipped to address the complexities of state-sponsored attacks, as they primarily focus on non-state actors and cross-border cybercrime.[3]

The challenges posed by state-sponsored cyberattacks are multifaceted, extending beyond technological considerations to issues of accountability, sovereignty, and justice. At the heart of these challenges lies the issue of attribution—the process of identifying the entity responsible for a cyberattack. In cyberspace, attackers can obscure their identities using techniques like spoofing, encryption, and the deployment of proxy actors. Even when technical evidence points to a specific actor, political and diplomatic considerations may prevent states from publicly attributing the attack. This ambiguity enables states to engage in malicious cyber activities with minimal risk of legal or diplomatic repercussions.[4]

Furthermore, the current international legal frameworks are ill-suited to address the specific nature of state-sponsored cyberattacks. The principles of state responsibility under customary international law require a high standard of proof to establish a state's involvement in malicious acts. However, in the context of cyberattacks, meeting this standard is often impractical due to the challenges of attribution. Additionally, the absence of a comprehensive international treaty specifically addressing cyber warfare and state-sponsored cyberattacks leaves a regulatory vacuum, making it difficult to define and prosecute such acts under existing legal frameworks.[5]

The lack of accountability for state-sponsored cyberattacks has significant implications for global security and the rule of law. It emboldens states to continue engaging in cyber operations without fear of consequences, undermining trust in international legal institutions and exacerbating geopolitical tensions. Without effective mechanisms to address these issues, the international community risks normalizing the use of cyberspace as a domain for unchecked state aggression.[6]

---

[2] William Akoto, "State-Sponsored Cyber Attacks and Co-Movements in Stock Market Returns: Evidence from US Cybersecurity Defense Contractors," *Business and Politics*, October 21, 2024, 1–19, https://doi.org/10.1017/bap.2024.22.
[3] Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017).
[4] Kristen Eichensehr, *The Law & Politics of Cyberattack Attribution*, 2019.
[5] William Banks, "Cyber Attribution and State Responsibility," *International Law Studies* 97, no. 1 (2021): 43.
[6] Eichensehr, *The Law & Politics of Cyberattack Attribution*.

To address the pressing issues surrounding state-sponsored cyberattacks, this research seeks to explore how international criminal law can more effectively respond to these threats, identify the gaps in current legal frameworks that hinder prosecution, and propose the necessary reforms to enhance accountability.[7] The primary objective of the study is to analyze the deficiencies within existing international legal instruments and frameworks that prevent effective accountability for state-sponsored cyberattacks. By examining existing treaties, customary international law, and case studies of state-backed cyber operations, the research will highlight the limitations of current legal instruments, such as the Budapest Convention, in addressing the complexities of cyberattacks. Additionally, it will propose legal and institutional reforms aimed at strengthening international accountability mechanisms and enhancing the understanding of the intersection between international criminal law and cyber operations.

This study will also explore the potential for expanding the jurisdiction of existing international bodies, such as the International Criminal Court (ICC), to include cybercrimes. It will consider the development of new treaties or agreements specifically designed to address the unique challenges posed by cyberspace. By tackling these issues, the research seeks to advance a more robust and comprehensive approach to international criminal accountability in the digital age. The rise of state-sponsored cyberattacks represents a significant challenge to the international legal order, as these attacks exploit the characteristics of cyberspace to evade accountability, thereby undermining global security and the rule of law. Through this research, we aim to bridge the gaps in international criminal law, offering a pathway toward greater accountability and justice in the face of evolving threats.

Research Method

This research takes a qualitative approach, combining case study analysis and legal review to examine the challenges in addressing state-sponsored cyberattacks. It focuses on high-profile incidents like Stuxnet and SolarWinds to explore issues of attribution and accountability. The study reviews existing legal instruments, including the Budapest Convention and the Tallinn Manual, to assess their effectiveness in addressing cyber threats, with a focus on jurisdiction and enforcement. Additionally, the research examines principles of state responsibility under customary international law and their application to cyberspace. Based on these analyses, the study proposes legal reforms to enhance accountability and improve international cooperation in tackling cyber warfare.[8]

[7] Peter Margulies, "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility," *Melbourne Journal of International Law* 14 (2015): 496.
[8] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.

Understanding State-Sponsored Cyberattacks

State-sponsored cyberattacks have emerged as a defining feature of modern conflicts, reflecting the increasing integration of cyberspace into global power dynamics. These attacks are characterized by their deliberate and coordinated nature, often carried out with the backing or direct involvement of state actors. They target critical infrastructure, disrupt political systems, and compromise national security, posing unique challenges to international stability and law enforcement.[9]

Definition, Characteristics, and Examples

State-sponsored cyberattacks can be broadly defined as malicious cyber activities executed by or on behalf of a nation-state to achieve strategic objectives. Unlike traditional cybercrimes driven by personal or financial motives, these attacks are inherently political, aimed at advancing a state's geopolitical, economic, or military interests. A key characteristic of such operations is their sophistication, often leveraging advanced technologies, zero-day vulnerabilities, and extensive resources unavailable to non-state actors.[10]

One of the most prominent examples of a state-sponsored cyberattack is the Stuxnet worm, discovered in 2010. Allegedly developed by the United States and Israel, Stuxnet was designed to sabotage Iran's nuclear enrichment program by targeting specific industrial control systems. This attack marked a turning point in cyber warfare, demonstrating the potential of cyber tools to inflict physical damage on critical infrastructure.[11]

Another notable case is the SolarWinds hack, uncovered in 2020, which compromised multiple U.S. government agencies and private sector organizations. Attributed to Russian state actors, the attack involved infiltrating widely used software to gain access to sensitive systems, highlighting the risks posed by supply chain vulnerabilities.[12] Similarly, the WannaCry ransomware attack in 2017, attributed to North Korean operatives, disrupted

[9] Eichensehr, *The Law & Politics of Cyberattack Attribution*.
[10] Callistus Francis AZUBUIKE, "Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks," *Nnamdi Azikiwe Journal of Political Science* 8, no. 3 (2023): 101–14.
[11] Patrick Butler et al., "Cybersecurity Threats: An Analysis of the Rise and Impacts of State Sponsored Cyber Attacks," in *Software Engineering Research and Practice and E-Learning, e-Business, Enterprise Information Systems, and e-Government*, ed. Hamid R. Arabnia and Leonidas Deligiannidis, Communications in Computer and Information Science (Cham: Springer Nature Switzerland, 2025), 2263:187–94, https://doi.org/10.1007/978-3-031-86644-9_14.
[12] Antonio Coco, Talita Dias, and Tsvetelina Van Benthem, "Illegal: The SolarWinds Hack under International Law," *European Journal of International Law* 33, no. 4 (December 2022): 1275–86, https://doi.org/10.1093/ejil/chac063.

healthcare and financial services globally, emphasizing the far-reaching consequences of state-sponsored operations.[13]

These cases underscore the unique attributes of state-sponsored cyberattacks: precision targeting, advanced technological capabilities, and the potential to cause widespread disruption. Unlike traditional acts of aggression, these operations are often conducted covertly, allowing states to deny involvement and avoid direct confrontation.

Impact and Challenges of Attribution

The impact of state-sponsored cyberattacks is profound, affecting national security, economic stability, and global trust. By targeting critical infrastructure such as power grids, financial systems, and communication networks, these attacks can paralyze essential services and erode public confidence in state institutions. For instance, the 2015 and 2016 cyberattacks on Ukraine's power grid, attributed to Russian actors, left hundreds of thousands of residents without electricity, demonstrating the tangible consequences of cyber operations.[14]

Beyond immediate disruptions, state-sponsored cyberattacks have broader geopolitical implications. They can escalate tensions between nations, undermine democratic processes, and create an atmosphere of mistrust. The alleged Russian interference in the 2016 U.S. presidential election, involving hacking and dissemination of disinformation, exemplifies how cyber operations can influence political outcomes and challenge the sovereignty of democratic states.[15]

Attribution remains one of the most significant challenges in addressing state-sponsored cyberattacks. Unlike traditional acts of aggression, where the perpetrator's identity is often clear, cyber operations allow attackers to mask their origins through techniques such as IP spoofing, encryption, and the use of proxy actors. This ambiguity complicates efforts to hold states accountable under international law.

Moreover, even when technical evidence points to a specific actor, the threshold for attribution under international law requires a high degree of certainty. States may be reluctant to publicly attribute attacks due to fears of escalating conflicts or revealing intelligence capabilities. This reluctance creates a permissive environment where states can engage in cyber operations with minimal risk of consequences.

---

[13] Sumaiah Algarni, "Cybersecurity Attacks: Analysis of 'WannaCry' Attack and Proposing Methods for Reducing or Preventing Such Attacks in Future," in *ICT Systems and Sustainability*, ed. Milan Tuba, Shyam Akashe, and Amit Joshi, Advances in Intelligent Systems and Computing (Singapore: Springer Singapore, 2021), 1270:763–70, https://doi.org/10.1007/978-981-15-8289-9_73.

[14] Vetrivel Subramaniam Rajkumar et al., "Cyber Attacks on Power Grids: Causes and Propagation of Cascading Failures," *IEEE Access* 11 (2023): 103154–76, https://doi.org/10.1109/ACCESS.2023.3317695.

[15] Radosław Fordoński and Wojciech Kasprzak, "Alleged Russian Interference in the 2016 US Presidential Election and Prohibition of Non-Intervention," *Radosław Fordoński, Wojciech Kasprzak, Alleged Russian Interference*, 2018, 113.

The complexity of attribution is further exacerbated by the use of non-state actors as proxies. States may outsource cyber operations to criminal groups or private contractors, creating a layer of plausible deniability. For instance, the Lazarus Group, linked to North Korea, has been implicated in numerous cyberattacks, including the WannaCry ransomware campaign, blurring the line between state and non-state activities.[16]

Addressing these challenges requires a combination of technological, legal, and diplomatic efforts. Advances in forensic technology and international cooperation can enhance attribution capabilities, while stronger legal frameworks can provide mechanisms for holding states accountable. However, achieving consensus on these measures remains a significant hurdle in the fragmented landscape of international law.

In conclusion, understanding state-sponsored cyberattacks involves recognizing their unique characteristics, analyzing their profound impacts, and addressing the challenges of attribution. As the digital domain becomes increasingly central to global power dynamics, the international community must develop comprehensive strategies to address these threats and uphold the principles of sovereignty and accountability.

Legal Frameworks and State Responsibility

The proliferation of state-sponsored cyberattacks has prompted urgent discussions on the adequacy of existing international legal frameworks and the principles governing state responsibility in cyberspace. This chapter delves into the current legal instruments designed to regulate cyber activities and examines the challenges inherent in applying state responsibility doctrines to the complex and evolving landscape of cyber operations.

Existing Legal Instruments

International law offers several frameworks aimed at addressing cyber activities, but their efficacy in dealing with state-sponsored cyberattacks is limited. Among the most significant instruments are the Budapest Convention on Cybercrime and the Tallinn Manual on the International Law Applicable to Cyber Warfare.

The Budapest Convention on Cybercrime, adopted in 2001 by the Council of Europe, is the first international treaty addressing crimes committed via the internet and other computer networks. It focuses on promoting international cooperation in combating cybercrime and provides a framework for harmonizing national laws. The convention's scope includes offenses such as illegal access, data interference, and system interference.[17] However, its

[16] Arif Perdana, Muhamad Erza Aminanto, and Bayu Anggorojati, "Hack, Heist, and Havoc: The Lazarus Group's Triple Threat to Global Cybersecurity," *Journal of Information Technology Teaching Cases*, December 4, 2024, 20438869241303941, https://doi.org/10.1177/20438869241303941.
[17] Lennon Y. C. Chang, "Legislative Frameworks Against Cybercrime: The Budapest Convention and Asia," in *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (Cham: Springer International Publishing, 2020), 1–17, https://doi.org/10.1007/978-3-319-90307-1_6-1.

application to state-sponsored cyberattacks is constrained by several factors. First, the convention primarily targets criminal activities conducted by individuals or non-state groups, rather than actions carried out or sponsored by states. Second, key cyber powers, such as Russia and China, have not ratified the Budapest Convention, reducing its global applicability and enforcement capabilities. Third, cybercrimes often transcend national borders, creating difficulties in determining jurisdiction and obtaining evidence across jurisdictions.[18]

The Tallinn Manual, first published in 2013 and updated in 2017, represents a significant effort to clarify how international law applies to cyber operations. Developed by legal experts under the auspices of NATO's Cooperative Cyber Defence Centre of Excellence, the manual provides a non-binding interpretation of existing laws, particularly in the context of armed conflict. It addresses key issues such as sovereignty, the use of force, and state responsibility in cyberspace. Despite its contributions, the Tallinn Manual faces several limitations. It is an academic study rather than a legally binding document, limiting its enforceability and influence on state behavior. Additionally, states differ in their interpretations of international law as it applies to cyberspace, leading to disagreements on the manual's principles and recommendations. Furthermore, the manual primarily addresses cyber operations in the context of warfare, leaving gaps in its applicability to peacetime cyberattacks.[19]

Beyond these instruments, other international agreements, such as the United Nations Charter and the Geneva Conventions, provide general principles that may be relevant to cyber activities. For instance, the prohibition on the use of force under Article 2(4) of the UN Charter could theoretically apply to cyberattacks causing physical damage or significant disruption. However, the absence of explicit provisions addressing cyber-specific issues limits the practical utility of these frameworks.[20]

The limitations of existing legal instruments highlight the challenges of regulating state-sponsored cyberattacks within the current international legal system. Key issues include enforcement and accountability, ambiguity, and geopolitical barriers. International law lacks effective mechanisms to enforce compliance and hold states accountable for cyberattacks.[21] The decentralized nature of the internet and the anonymity it affords further complicate enforcement efforts. Additionally, the lack of universally accepted

[18] Antonio Segura-Serrano, ed., *Global Cybersecurity and International Law*, Routledge Research in IT and E-Commerce Law (London ; New York: Routledge Taylor & Francis Group, 2024).
[19] Ebru Oğurlu, "International Law in Cyberspace: An Evaluation of the Tallinn Manuals," *Annales de La Faculté de Droit d'Istanbul* 0, no. 73 (November 2023): 327–44, https://doi.org/10.26650/annales.2023.73.0010.
[20] Su Yuting and Jiang Shengli, "International Legal Framework for Cyber Attacks in Outer Space:The Issue of 'Use of Force,'" *US-China Law Review* 22, no. 2 (February 2025), https://doi.org/10.17265/1548-6605/2025.02.003.
[21] M. M. Rahman and T. K. Das, "Countering Cyberattacks: Gaps in International Law and Prospects for Overcoming Them," *Journal of Digital Technologies and Law* 2, no. 4 (December 2024): 973–1002, https://doi.org/10.21202/jdtl.2024.46.

definitions for terms such as "cyber warfare" and "cyber aggression" creates ambiguity, making it difficult to determine when an act constitutes a violation of international law. Efforts to develop new legal instruments are often hindered by geopolitical tensions and differing national interests. Powerful states may resist constraints on their cyber capabilities, further delaying progress.

State Responsibility in Cyberspace

The principle of state responsibility is a cornerstone of international law, encapsulated in the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA). These articles establish that states are responsible for internationally wrongful acts attributable to them and outline the legal consequences of such acts, including reparations and cessation. Applying these principles to cyberspace, however, presents unique challenges.

Attribution is a critical component of establishing state responsibility for cyberattacks. Under international law, a state can be held accountable if the act is carried out by state organs or entities exercising governmental authority or if non-state actors act under the direction or control of the state. In cyberspace, attribution is particularly challenging due to the anonymity of cyber operations and the use of sophisticated techniques to obfuscate origins. States may employ proxies, such as criminal groups or private contractors, to carry out attacks, creating plausible deniability. For example, the Lazarus Group, linked to North Korea, has conducted cyberattacks with significant geopolitical implications, blurring the line between state and non-state actions.[22]

Technological advancements, such as digital forensics and threat intelligence, have improved attribution capabilities, but they often fall short of meeting the high evidentiary standards required under international law. Furthermore, states may be reluctant to publicly attribute attacks due to concerns about revealing intelligence capabilities or escalating conflicts.

While ARSIWA provides a general framework for state responsibility,[23] its application to cyberspace is fraught with difficulties. Many cyberattacks do not cause physical damage but can have significant economic, political, or psychological impacts.[24] Determining whether such acts constitute a violation of international law is often contentious. The UN Charter prohibits the use of force except in cases of self-defense or with Security Council authorization. Applying this principle to cyberattacks is challenging, as the threshold for what constitutes "force" in cyberspace remains unclear. Principles of proportionality and necessity, which govern state responses to wrongful acts, are also difficult to apply in the

[22] James A Lewis, *Creating Accountability for Global Cyber Norms*, JSTOR, 2022.
[23] Jane Hofbauer and Philipp Janig, "State Responsibility," *Elgar Encyclopedia of Human Rights (2022)*, 2022.
[24] Martti Lehto, "Cyber-Attacks Against Critical Infrastructure," in *Cyber Security*, ed. Martti Lehto and Pekka Neittaanmäki, Computational Methods in Applied Sciences (Cham: Springer International Publishing, 2022), 56:3–42, https://doi.org/10.1007/978-3-030-91293-2_1.

cyber context. Determining an appropriate and proportionate response to a cyberattack involves complex considerations of intent, impact, and attribution.

The involvement of non-state actors in state-sponsored cyber operations further complicates the application of state responsibility principles. States may provide financial support, training, or resources to such actors, effectively outsourcing cyberattacks while maintaining plausible deniability. This practice challenges traditional notions of state accountability and necessitates a reevaluation of legal doctrines to address the unique dynamics of cyberspace.

Despite the existence of principles governing state responsibility, the international community lacks clear mechanisms for holding states accountable for cyberattacks. The International Court of Justice (ICJ) and other judicial bodies have limited jurisdiction over cyber-related disputes, and political considerations often undermine efforts to pursue legal remedies. Additionally, the fragmented nature of international law in cyberspace creates opportunities for states to exploit legal loopholes.[25]

The existing legal frameworks and principles of state responsibility provide a foundation for addressing state-sponsored cyberattacks, but significant gaps and challenges remain. The limitations of current treaties, the complexities of attribution, and the involvement of non-state actors highlight the need for a more robust and tailored approach. As cyberspace continues to evolve as a domain of conflict and competition, the international community must prioritize the development of comprehensive legal instruments and mechanisms that address the unique characteristics of cyber operations while upholding the principles of sovereignty and accountability.

Bridging the Gaps and Future Directions

The rapidly evolving nature of cyberspace as a domain of conflict and criminal activity underscores the urgent need to address the gaps in existing legal frameworks and enforcement mechanisms. As state-sponsored cyberattacks become increasingly sophisticated and impactful, the international community must explore comprehensive reforms, strengthen mechanisms for attribution and enforcement, and consider the ethical and political dimensions of these efforts. This chapter outlines proposed reforms, mechanisms to enhance enforcement, ethical challenges, and lessons learned from historical case studies.

[25] Md Nazrul Islam Khan and Ishtiaque Ahmed, "A Systematic Review of Judicial Reforms and Legal Access Strategies in the Age of Cybercrime and Digital Evidence," *International Journal of Scientific Interdisciplinary Research* 05, no. 02 (June 2024): 01–29, https://doi.org/10.63125/96ex9767.

Proposed Reforms

Efforts to bridge the gaps in the current legal framework for addressing cyberattacks require targeted reforms to adapt international law to the unique challenges of cyberspace. Two significant proposals include expanding the jurisdiction of the International Criminal Court (ICC) and developing new treaties specific to cyber warfare and cybercrimes.

One of the most ambitious reforms would involve expanding the jurisdiction of the International Criminal Court to encompass cybercrimes. The ICC's mandate currently includes grave offenses such as genocide, war crimes, and crimes against humanity. Including cybercrimes, particularly those involving state-sponsored attacks on critical infrastructure or large-scale violations of human rights, would represent a significant step forward. Such a reform would require amending the Rome Statute, the treaty that established the ICC, to explicitly define cybercrimes and delineate the court's jurisdiction over these offenses. Challenges to this proposal include securing consensus among member states, addressing concerns about sovereignty, and ensuring that the ICC has the technical expertise to adjudicate cyber-related cases.[26]

In addition to ICC expansion, the development of new international treaties specifically tailored to cyber warfare and cybercrimes is imperative. Existing instruments, such as the Budapest Convention, provide a foundation but fall short in addressing state-sponsored operations and cyber conflicts. A new treaty could establish universally accepted definitions of cyber warfare, delineate thresholds for the use of force in cyberspace, and create protocols for cooperation in investigations and enforcement. Such a treaty would also need to address critical issues like sovereignty, proportionality, and the involvement of non-state actors. Negotiating such an agreement would require overcoming significant geopolitical obstacles, particularly resistance from major cyber powers wary of limiting their operational capabilities.[27]

Strengthening Mechanisms for Attribution and Enforcement

Enhancing the mechanisms for attributing cyberattacks to their perpetrators and enforcing legal consequences is essential for holding actors accountable and deterring future incidents. Key strategies include leveraging forensic technology, promoting international cooperation, imposing sanctions, and strengthening the role of international organizations.

Advancements in forensic technology play a critical role in improving attribution capabilities. Techniques such as digital fingerprinting, machine learning-based analysis, and real-time monitoring of cyber activities enable investigators to trace attacks back to

[26] Maruf Billah, "Prosecuting Crimes against Humanity and Genocide at the International Crimes Tribunal Bangladesh: An Approach to International Criminal Law Standards," *Laws* 10, no. 4 (October 2021): 82, https://doi.org/10.3390/laws10040082.
[27] Michael R. Kenwick and Douglas Lemke, "International Influences on the Survival of Territorial Non-State Actors," *British Journal of Political Science* 53, no. 2 (April 2023): 479–97, https://doi.org/10.1017/S0007123422000333.

their sources with greater precision.[28] However, technical attribution alone is insufficient without international cooperation. Governments, private sector entities, and international organizations must collaborate to share intelligence, pool resources, and establish common standards for evidence collection and analysis.

Enforcement mechanisms must also include sanctions and legal consequences for state-sponsored cyber operations. Economic sanctions, travel bans, and diplomatic measures can serve as deterrents for states engaging in malicious cyber activities. For instance, coordinated sanctions imposed by the United States and the European Union have been effective in penalizing entities responsible for cyberattacks attributed to state actors.[29] However, sanctions must be accompanied by legal remedies to address the harm caused by such attacks. This could involve establishing specialized international tribunals for cybercrimes or integrating cyber-specific provisions into existing judicial bodies.

The United Nations and other international organizations have a crucial role to play in enforcing accountability for cyberattacks. The UN could facilitate the development of a global framework for cyber conflict resolution, including mechanisms for mediation and arbitration. Moreover, specialized agencies, such as the International Telecommunication Union (ITU), can contribute technical expertise and capacity-building support to member states. Enhancing the UN's role in cyber governance would require addressing structural challenges, such as the veto power held by permanent Security Council members, which often stymies collective action.

Ethical and Political Considerations

Efforts to strengthen the legal and enforcement mechanisms for addressing cyberattacks must account for the ethical and political dimensions of these initiatives. Balancing state sovereignty with the need for accountability and navigating the geopolitical implications of legal reforms are particularly critical.

One of the central ethical challenges lies in balancing sovereignty with accountability.[30] States have a legitimate interest in protecting their sovereignty and maintaining control over their cyber infrastructures. However, unchecked sovereignty can lead to a lack of accountability for cyber operations that violate international law. Legal frameworks must strike a balance between respecting state autonomy and ensuring that states are held accountable for wrongful acts. This includes addressing the potential misuse of legal

[28] Bandr Fakiha, "Enhancing Cyber Forensics with AI and Machine Learning: A Study on Automated Threat Analysis and Classification," *International Journal of Safety and Security Engineering* 13, no. 4 (September 2023): 701–7, https://doi.org/10.18280/ijsse.130412.
[29] Vera Rusinova and Ekaterina Martynova, "Fighting Cyber Attacks with Sanctions: Digital Threats, Economic Responses," *Israel Law Review* 57, no. 1 (March 2024): 135–74, https://doi.org/10.1017/S0021223722000255.
[30] Niël Henk Conradie and Saskia K. Nagel, "Digital Sovereignty and Smart Wearables: Three Moral Calculi for the Distribution of Legitimate Control over the Digital," *Journal of Responsible Technology* 12 (December 2022): 100053, https://doi.org/10.1016/j.jrt.2022.100053.

instruments to suppress dissent or target political adversaries under the guise of cybersecurity enforcement.

The geopolitical implications of cyber governance reforms present additional challenges. Major cyber powers, such as the United States, China, and Russia, often have conflicting interests that hinder consensus on international norms and agreements. Resistance from powerful states may stem from concerns about limiting their cyber capabilities or ceding influence in the global digital arena.[31] Moreover, political biases and double standards in the enforcement of cyber norms could undermine the legitimacy of international legal instruments. To navigate these complexities, reforms must emphasize inclusivity, transparency, and equitable treatment of all states.

Case Studies and Lessons Learned

Analyzing historical incidents and their outcomes provides valuable insights into the challenges and opportunities associated with addressing state-sponsored cyberattacks. Two notable examples illustrate these dynamics: the 2014 Sony Pictures hack and the 2017 NotPetya attack.

The Sony Pictures hack, attributed to North Korea, involved the theft and public release of sensitive data in retaliation for the release of a film critical of the regime. The incident highlighted the challenges of attributing cyberattacks to state actors and the limited options for enforcement. In response, the United States imposed sanctions on North Korean individuals and entities, demonstrating the utility of targeted economic measures. However, the hack also underscored the need for stronger international cooperation to deter similar incidents in the future.[32]

The NotPetya attack, widely attributed to Russian actors, was a devastating ransomware campaign that caused billions of dollars in damages worldwide. Initially targeting Ukrainian infrastructure, the attack quickly spread to other countries, affecting businesses and government agencies. The incident exposed the vulnerabilities of interconnected global networks and the potential for collateral damage in cyber conflicts. It also highlighted the limitations of existing legal frameworks in addressing cross-border cyber incidents. International responses to NotPetya, including sanctions and public

[31] Mischa Hansel, "Great Power Narratives on the Challenges of Cyber Norm Building," *Policy Design and Practice* 6, no. 2 (April 2023): 182–97, https://doi.org/10.1080/25741292.2023.2175995.
[32] Ngozi Tracy Aleke, Ivan Livingstone Zziwa, and Kwame Opoku-Appiah, "Nation-State Cyber Attacks on Critical Infrastructure: A Case Study and Analysis of the 2014 Sony Pictures Hack by North Korea," in *Advances in Information Security, Privacy, and Ethics*, ed. Hewa Majeed Zangana and Marwan Omar (IGI Global, 2025), 143–68, https://doi.org/10.4018/979-8-3373-1102-9.ch005.

attributions, underscored the importance of coordinated action but also revealed gaps in enforcement mechanisms. [33]

These case studies emphasize the need for comprehensive reforms that address the technical, legal, and political dimensions of cyberattacks. Lessons learned from prior incidents can inform the development of more effective frameworks for prevention, attribution, and accountability.

Conclusion

The analysis presented underscores the urgent need for robust international frameworks to address the rising threat of state-sponsored cyberattacks and cybercrimes. Existing legal instruments, while foundational, remain inadequate to tackle the complexities of cyberspace, particularly concerning enforcement, jurisdiction, and accountability. Proposals for expanding the ICC's jurisdiction and drafting new treaties signify promising steps forward, complemented by advancements in forensic technology and international cooperation. However, ethical considerations, including the balance between sovereignty and accountability, and geopolitical dynamics, highlight the challenges in achieving global consensus. Historical case studies such as the Sony Pictures hack and the NotPetya attack emphasize the importance of learning from past incidents to shape future strategies. A multi-faceted approach that integrates legal reforms, technological advancements, and ethical considerations is essential. Only through sustained collaboration and innovation can the international community ensure a secure and equitable cyberspace for all stakeholders.

Acknowledgment

None

Conflict of Interest

There are no relevant financial or non-financial competing interests to report.

Author(s) Contribution

Author 1: initiated the research ideas, instrument construction, data collection, analysis, and draft writing.

[33] Annegret Bendiek and Matthias Schulze, "Attribution: A Major Challenge for EU Cyber Sanctions: An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW," *SWP Research Paper*, Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs, 2021, 11/2021, https://doi.org/10.18449/2021RP11.

References

Akoto, William. "State-Sponsored Cyber Attacks and Co-Movements in Stock Market Returns: Evidence from US Cybersecurity Defense Contractors." *Business and Politics*, October 21, 2024, 1–19. https://doi.org/10.1017/bap.2024.22.

Aleke, Ngozi Tracy, Ivan Livingstone Zziwa, and Kwame Opoku-Appiah. "Nation-State Cyber Attacks on Critical Infrastructure: A Case Study and Analysis of the 2014 Sony Pictures Hack by North Korea." In *Advances in Information Security, Privacy, and Ethics*, edited by Hewa Majeed Zangana and Marwan Omar, 143–68. IGI Global, 2025. https://doi.org/10.4018/979-8-3373-1102-9.ch005.

Algarni, Sumaiah. "Cybersecurity Attacks: Analysis of 'WannaCry' Attack and Proposing Methods for Reducing or Preventing Such Attacks in Future." In *ICT Systems and Sustainability*, edited by Milan Tuba, Shyam Akashe, and Amit Joshi, 1270:763–70. Advances in Intelligent Systems and Computing. Singapore: Springer Singapore, 2021. https://doi.org/10.1007/978-981-15-8289-9_73.

AZUBUIKE, Callistus Francis. "Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks." *Nnamdi Azikiwe Journal of Political Science* 8, no. 3 (2023): 101–14.

Banks, William. "Cyber Attribution and State Responsibility." *International Law Studies* 97, no. 1 (2021): 43.

Bendiek, Annegret, and Matthias Schulze. "Attribution: A Major Challenge for EU Cyber Sanctions: An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW." *SWP Research Paper*, Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs, 2021, 11/2021. https://doi.org/10.18449/2021RP11.

Billah, Maruf. "Prosecuting Crimes against Humanity and Genocide at the International Crimes Tribunal Bangladesh: An Approach to International Criminal Law Standards." *Laws* 10, no. 4 (October 2021): 82. https://doi.org/10.3390/laws10040082.

Butler, Patrick, Jayden Kelley, Juston Ellis, and Samuel Olatunbosun. "Cybersecurity Threats: An Analysis of the Rise and Impacts of State Sponsored Cyber Attacks." In *Software Engineering Research and Practice and E-Learning, e-Business, Enterprise Information Systems, and e-Government*, edited by Hamid R. Arabnia and Leonidas Deligiannidis, 2263:187–94. Communications in Computer and Information Science. Cham: Springer Nature Switzerland, 2025. https://doi.org/10.1007/978-3-031-86644-9_14.

Chang, Lennon Y. C. "Legislative Frameworks Against Cybercrime: The Budapest Convention and Asia." In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 1–17. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-319-90307-1_6-1.

Coco, Antonio, Talita Dias, and Tsvetelina Van Benthem. "Illegal: The SolarWinds Hack under International Law." *European Journal of International Law* 33, no. 4 (December 2022): 1275–86. https://doi.org/10.1093/ejil/chac063.

Conradie, Niël Henk, and Saskia K. Nagel. "Digital Sovereignty and Smart Wearables: Three Moral Calculi for the Distribution of Legitimate Control over the Digital." *Journal of Responsible Technology* 12 (December 2022): 100053. https://doi.org/10.1016/j.jrt.2022.100053.

Durojaye, Henry, and Oluwaukola Raji. "Impact of State and State Sponsored Actors on the Cyber Environment and the Future of Critical Infrastructure." Version 1. Preprint, arXiv, 2022. https://doi.org/10.48550/ARXIV.2212.08036.

Eichensehr, Kristen. *The Law & Politics of Cyberattack Attribution*. 2019.

Fakiha, Bandr. "Enhancing Cyber Forensics with AI and Machine Learning: A Study on Automated Threat Analysis and Classification." *International Journal of Safety and Security Engineering* 13, no. 4 (September 2023): 701–7. https://doi.org/10.18280/ijsse.130412.

Fordoński, Radosław, and Wojciech Kasprzak. "Alleged Russian Interference in the 2016 US Presidential Election and Prohibition of Non-Intervention." *Radosław Fordoński, Wojciech Kasprzak, Alleged Russian Interference*, 2018, 113.

Hansel, Mischa. "Great Power Narratives on the Challenges of Cyber Norm Building." *Policy Design and Practice* 6, no. 2 (April 2023): 182–97. https://doi.org/10.1080/25741292.2023.2175995.

Hofbauer, Jane, and Philipp Janig. "State Responsibility." *Elgar Encyclopedia of Human Rights (2022)*, 2022.

Kenwick, Michael R., and Douglas Lemke. "International Influences on the Survival of Territorial Non-State Actors." *British Journal of Political Science* 53, no. 2 (April 2023): 479–97. https://doi.org/10.1017/S0007123422000333.

Khan, Md Nazrul Islam, and Ishtiaque Ahmed. "A Systematic Review of Judicial Reforms and Legal Access Strategies in the Age of Cybercrime and Digital Evidence." *International Journal of Scientific Interdisciplinary Research* 05, no. 02 (June 2024): 01–29. https://doi.org/10.63125/96ex9767.

Lehto, Martti. "Cyber-Attacks Against Critical Infrastructure." In *Cyber Security*, edited by Martti Lehto and Pekka Neittaanmäki, 56:3–42. Computational Methods in Applied Sciences. Cham: Springer International Publishing, 2022. https://doi.org/10.1007/978-3-030-91293-2_1.

Lewis, James A. *Creating Accountability for Global Cyber Norms*. JSTOR, 2022.

Margulies, Peter. "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility." *Melbourne Journal of International Law* 14 (2015): 496.

Oğurlu, Ebru. "International Law in Cyberspace: An Evaluation of the Tallinn Manuals." *Annales de La Faculté de Droit d'Istanbul* 0, no. 73 (November 2023): 327–44. https://doi.org/10.26650/annales.2023.73.0010.

Perdana, Arif, Muhamad Erza Aminanto, and Bayu Anggorojati. "Hack, Heist, and Havoc: The Lazarus Group's Triple Threat to Global Cybersecurity." *Journal of Information Technology Teaching Cases*, December 4, 2024, 20438869241303941. https://doi.org/10.1177/20438869241303941.

Rahman, M. M., and T. K. Das. "Countering Cyberattacks: Gaps in International Law and Prospects for Overcoming Them." *Journal of Digital Technologies and Law* 2, no. 4 (December 2024): 973–1002. https://doi.org/10.21202/jdtl.2024.46.

Rajkumar, Vetrivel Subramaniam, Alexandru Ștefanov, Alfan Presekal, Peter Palensky, and José Luis Rueda Torres. "Cyber Attacks on Power Grids: Causes and Propagation of Cascading Failures." *IEEE Access* 11 (2023): 103154–76. https://doi.org/10.1109/ACCESS.2023.3317695.

Rusinova, Vera, and Ekaterina Martynova. "Fighting Cyber Attacks with Sanctions: Digital Threats, Economic Responses." *Israel Law Review* 57, no. 1 (March 2024): 135–74. https://doi.org/10.1017/S0021223722000255.

Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017.

Segura-Serrano, Antonio, ed. *Global Cybersecurity and International Law*. Routledge Research in IT and E-Commerce Law. London ; New York: Routledge Taylor & Francis Group, 2024.

Su Yuting and Jiang Shengli. "International Legal Framework for Cyber Attacks in Outer Space:The Issue of 'Use of Force.'" *US-China Law Review* 22, no. 2 (February 2025). https://doi.org/10.17265/1548-6605/2025.02.003.