International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18 (2026) pp. 1-12

https://doi.org/10.70917/ijcisim-2026-0090
Article

International Law and The Regulation of Cross-Border Cyberattacks: Challenges and Solutions

Xuejiao Qu *

School of Humanities and Social Sciences, Harbin Engineering University, Harbin, Heilongjiang, 150001, China; quxj225@163.com

Abstract: In response to the global governance challenges posed by cross-border cyberattacks, this paper discusses the legal liability standards for cross-border cyberattacks, the conditions for the application of a state's "right to self-defense," and the pathways for the application of international law. Based on this, the author proposes establishing a "two-tier liability standard" system to address increasingly complex cyberattacks, while introducing the principle of "duty of care for cross-border harm" as a supplementary liability pathway to establish a logically consistent liability mechanism. The author proposes that the "effective control" standard applies to general cyberattacks, the "full control" standard applies to cyberattacks with characteristics of armed conflict, and the "duty of care" principle serves as a fallback mechanism. To address the aforementioned challenges, the author advocates a dual-track system for the application of international law—a complementary and mutually reinforcing model—specifically, the complementary integration of "hard law and soft law, international rules and domestic laws, and multilateral mechanisms and bilateral coordination mechanisms." Regarding China's role and position in cyberattack governance, the author suggests that China should promote the concept of a "community of shared future in cyberspace" based on the principles of "equality, innovation, openness, and sharing" by actively safeguarding its own cyber interests as a leading factor (positive form). This approach ensures that national sovereignty is upheld while facilitating smooth international cooperation, maintaining a balanced relationship. This study addresses the research gap in the application of international law in cyberspace and provides a research basis and policy recommendations for states conducting cross-border cyberattacks, thereby advancing the establishment of legal norms in cyberspace.

Keywords: cross-border cyberattacks; international law; liability standards; right of self-defense; cyberspace governance

1. Introduction

The advent of the digital age has transformed cyberspace into a new frontier beyond land, sea, air, and space. From government to private enterprises, and from social media to the financial sector, the influence of cyberspace has fundamentally reshaped the traditional ways in which states exercise sovereignty and define national borders [1-3]. In contrast, unlike traditional territorial states, the covert nature, difficulty in tracing, and rapid spread of cyberattacks have left traditional international law ill-equipped to address this new threat [4]. Especially as cyberattacks between nations intensify, their substantive impacts transcend purely technical dimensions and are closely intertwined with national security, international relations, and global governance [5-6]. Under the traditional international legal framework, the principles of "state responsibility," "state capacity," and "the inviolability of state sovereignty" are central. However, the perpetrators of cyberattacks can utilize facilities in other countries across different continents and employ technical means to sever the chain of attribution between nations [7-8]. The transition from "visible weapons" to "invisible code commands" underscores the urgent need for the traditional international legal framework to adapt to the digital age [9]. The first priority in revising international law on cybersecurity is to address the issue of a state's responsibility toward the

victim state, followed by the application of the principle of legitimate self-defense [10-11]. Especially for non-state actors, which frequently serve as attackers, the existing rule system is no longer sufficient [12-13]. “Moreover, there are significant differences among countries in the exercise of the right to self-defense against cyberattacks, with conflicting rules and political maneuvering intertwined, hindering the achievement of international cooperation consensus” [14-15]. It is imperative to establish an international regulatory system suitable for the digital age, strengthen the regulatory framework for cross-border cyberattacks, and maintain stability in the international cyberspace.

Literature [16] points out that to address cybersecurity issues, international law enforcement agencies need to develop and implement more comprehensive response measures, control and defense systems, and cybersecurity devices to ensure national security. Literature [17] notes that early international laws were drafted by officials over a decade ago, focusing on international political actors and neglecting control over cyberspace. Additionally, relevant international law enforcement agencies lack enforcement capacity, and the drafters exhibited some subjectivity, leading to inconsistencies in aligning self-interest with national interests. Literature [18] reports that the international binding treaties proposed by China and Russia have not been recognized by other countries. Nations lack specific interpretations and expressions of views on controversial legal issues in international cybersecurity. The challenge is not the difficulty in addressing these issues but the attempt to use vague norms to overreach, creating a hostile environment that poses significant challenges to the formulation of international law on transnational cyberattacks. Literature [19] analyzes that while the United Nations has reached consensus on a series of norms regarding the attribution of responsibility for cyberattacks, norm (f) is not suitable for prohibiting cyberattacks targeting critical infrastructure. This is due to both the inherent characteristics of such infrastructure and the contradictory legal status of norm (f), which in turn exacerbates the uncertainty of existing international laws regarding cyberspace. Literature [20] points out that in cyberspace, a country accused of engaging in harmful activities in cyberspace is unlikely to engage in serious self-reflection but will instead reject the accusations outright. This is because current international law lacks sufficient binding power over such accused countries, yet the accusations themselves may pave the way for new normative possibilities within the international community.

This paper selects cross-border cyberattacks as its research theme, aiming to explore the issue from three aspects: the elements of liability under international law, the exercise of the right to self-defense, and the implementation of international law. It proposes the following theoretical and practical approaches:

First, in the liability determination phase, starting from the existing theories of state responsibility underlying cross-border cyberattacks, a new, operationally feasible liability standard system should be constructed. Given the differences between cross-border cyberattacks and general attacks, the standards of “effective control” and “full control” are not suitable as primary liability norms, and their applicability in cyberspace should be explored.

Second, in the context of the initiation of self-defense, addressing issues such as the ambiguity of standards for assessing the consequences of cyber attacks, a multi-tiered, multi-perspective standard framework should be proposed for the exercise of the right to self-defense. This framework should comprehensively consider standards related to the consequences of attacks, the attacking entity (state), and strategic objectives, thereby mitigating the legal risks of abuse of preemptive self-defense in cyberspace.

Third, in terms of the implementation of international law rules, it is recommended to use soft law, domestic law, and multilateral mechanisms as complementary means to actively achieve the effective implementation and transformation of international law in cyberspace under the international law succession model.

2. Addressing International Law and Cross-Border Cyberattack Methods

2.1. Literature Analysis Method

Based on the research methodology outlined in this paper, the author first employs a literature review approach to explore the theoretical foundations of cross-border cyberattacks. The author examines the United Nations Charter as the legal source for cyberattacks and general legal liability, the Draft Articles on State Responsibility (hereinafter referred to as the “International Law Commission Draft”) as the specific legal provisions and basis for implementing cyberattacks, the International Convention for the Suppression of the Financing of Terrorism (hereinafter referred to as the “Cybercrime Convention”) as the specific provisions and basis for implementing cyberattacks, the “Draft Convention on the Prevention of Remote Intrusion into Computer Systems and Communication Systems in Developing Countries” (hereinafter referred to as the “Remote Intrusion Convention Draft”), which serves as an independent legislative document on cyberattacks, and materials such as “The Future Development of Space Law”

and “The Moral Philosophical Foundation of Choosing or Rejecting the International Convention on Information and Communication Technology: Theory and Practice,” which serve as research materials on cyberattacks, to establish the basis for analyzing cyberattacks. Analyze China's stance on the aforementioned laws and materials, as well as the positive significance of recognizing China's resolutions in the “International Law Commission Draft.” Promote the formulation and improvement of the “Cybercrime Convention,” the “Draft Convention on Remote Access,” and the upcoming international cybersecurity document—the “International Cybersecurity Law.” In the context of the heated debate in China over the use of proactive defensive measures to address cybersecurity threats and the U.S. National Security Agency (NSA) incident, China has adopted a different “attitude” to articulate its position.

Case law analysis constitutes the core component of literature analysis. Although international case law directly involving cyberattacks is relatively scarce, relevant case law from traditional international law provides us with rules and principles worthy of reference. We focus on analyzing the “effective control” standard established by the International Court of Justice in the “Nicaragua Case,” the “total control” standard developed by the International Criminal Tribunal in the “Tadić Case,” as well as the principles of due diligence and allocation of the burden of proof regarding cross-border harm established in the “Uruguay River Pulp Mill Case.” Typical cyberattack incidents such as the 2007 cyberattack on Estonia and the 2010 Stuxnet virus attack on Iran's nuclear facilities, along with their handling processes and international responses, are also included in our analysis. As an important supplement, we systematically studied the cybersecurity strategies, international cyberspace strategies, and position statements made by major countries such as the United States, Russia, and China in the United Nations Group of Governmental Experts. The United States' “International Cyberspace Strategy” emphasizes that existing international law is fully applicable to cyberspace. France's Ministry of Defense position paper explicitly supports the application of preemptive self-defense under specific conditions. China, meanwhile, emphasizes the importance of the principles of cyber sovereignty and peaceful development. Through comparative analysis of the commonalities and differences in the positions of various countries, we reveal the essential characteristics and development trends of the international rule-making dynamics in cyberspace.

2.2. Case Study Method

The “effective control” standard established by the International Court of Justice in the Nicaragua case requires proof of decisive control by a state over non-state actors engaged in specific acts, making it very difficult to attribute responsibility for cyber attacks, as it requires proof of “full control” by the state over the unlawful acts of non-state actors [21]. In contrast, the “sufficient control” standard adopted by the International Criminal Tribunal in the Tadić case significantly lowers the attribution threshold, as it only requires proof that the state exercised control over the overall planning and sponsorship of the armed conflict, rather than over specific acts [22]. These two standards fundamentally distinguish the divergent standards applied in cyberattack attribution practices, which require specific analysis based on the nature of the attack. The Corfu Channel case provides an important legal precedent for the implementation of the principle of due diligence in cyberattacks. The principle established in the Corfu Channel case that “every state has an obligation not to allow its territory to be used for activities that violate the rights of other states” is significant [23]. Even if it cannot be proven that a state directly controlled a cyberattack, it can still be held liable for failing to fulfill its duty to prevent such attacks. The Uruguay River Pulp Mill case corresponds to the development of the duty of care for cross-border harm, clarifying the possible forms of the duty of care, namely risk assessment, notification, and monitoring. This has implications for the determination of state responsibility in cyberspace by relevant international organizations [24].

The International Court of Justice's definition of “armed attack” in the China Oil Platform Case, namely “scale and impact,” has been adopted in the Tallinn Manual 2.0 and applied in the assessment of cyber operations. The definition of the boundaries of the right to self-defense in the Nicaragua Case also serves as a reference in assessing the application of the right to self-defense in cyber attacks. The principles of necessity and limitation in the Caroline case have practical guiding significance in restricting the abuse of preemptive self-defense in cyberspace [25]. Through case analyses of real-world cyberattacks such as the 2007 large-scale distributed denial-of-service attack on Estonia, the 2010 Stuxnet virus attack on Iran's nuclear facilities, and the 2016 hacking of the U.S. Democratic National Committee, we found that none of these incidents were resolved through judicial proceedings to determine the nature of the actions. However, through the corresponding measures and legal evaluations of various countries in the international community, it is also possible to discern the practical judgments made by the international community regarding the legal nature of cyberattacks. In this study, by integrating classical precedents with real-world cases, we have constructed a more comprehensive and

systematic legal framework for attributing responsibility for cyberattacks and the application of the right to self-defense, thereby overcoming the shortcomings of traditional analogical interpretations based solely on classical precedents.

2.3. Comparative Research Method

The significant differences in policy attitudes between the United States and Russia regarding cyberattack governance provide a window into the complex landscape of international rule-making for cross-border cyberattacks, offering insights for China's understanding of this issue [26]. The governance perspective outlined in the United States' "International Cyberspace Strategy" is characterized by strong advocacy and significant practical implementation. It states that cyberspace should not deviate from the framework of existing international law. However, the Strategy blurs the distinction between the concepts of "use of force" and "forceful attack," effectively lowering the threshold for exercising the right to self-defense, implying that forceful retaliation against cyberattacks can be justified under the principle of self-defense. Russia's governance perspective is, to a certain extent, the opposite of the United States'. First, Russia upholds cyber sovereignty, asserting that cyber sovereignty grants nations the right to regulate their own cyber infrastructure and information flow, and that traditional concepts of force should not be blindly applied to cyberspace. China's proposed "cyberspace community of shared future" governance concept embodies a balanced approach that prioritizes both security and development, actively pursuing international cooperation while upholding cyber sovereignty. EU member states adopt a relatively conventional approach to cyberattack governance. France asserts that the attacking party has a preemptive right based on self-defense, but cautiously limits this to situations where a cyberattack is "imminent"—a relatively extreme scenario. Germany seeks to resolve cyberspace disputes through multilateral frameworks. The Netherlands, however, adopts a very low standard of evidence for attributing cyberattacks.

The comparative standards established by the Tallinn Manual 2.0 for the application of the right to self-defense against cyberattacks serve as a reference for academia to determine whether such a right can be asserted. The Tallinn Manual defines the criteria for distinguishing between cyber behavior constituting an armed attack and non-armed attack as scale and effect, and acknowledges that the right to self-defense may be exercised against cyber behavior by terrorist organizations that reach the level of an armed attack. However, there are significant differences among countries in their understanding and application of these standards. Developed countries, as holders of advanced technological capabilities, often adopt flexible standards, while developing countries, especially those that may be targets of cyberattacks, tend to adopt strict standards. The National Computer Network Emergency Response Technical Team Coordination Center of China has monitored that 97.1% of active distributed denial-of-service attack control endpoints originate from abroad, primarily from the United States, Germany, the Netherlands, and other countries. This data not only highlights the extraterritorial nature of cyberattacks but also underscores the impact of uneven distribution of cyber capabilities on the shaping of international cyberattack rules. Regional organizations' governance experiences within the cyberattack domain offer multi-dimensional comparisons. The Association of Southeast Asian Nations (ASEAN) has addressed cyber issues by bridging regional differences and strengthening regional identity, establishing a cyber governance coordination framework that is led by governance matters and open to participation from all stakeholders through top-down and bottom-up interactions [27].

2.4. Empirical Analysis Method

Quantitative research methods serve as the theoretical foundation for research supported by concrete material data. For studies on the formulation of international legal rules regarding cross-border cyberattacks, such methods provide an indispensable material foundation. This paper explores three dimensions: quantitative analysis of International Court of Justice data, statistical support from cyberattack and defense technology data, and empirical evidence of the effectiveness of rule application under international law. These efforts aim to provide support for the extraction and utilization of cyberattack and defense data. Regarding the long-standing debate over control standards in the "Nicaragua Case" and the "Tadić Case," after reviewing established cases, it was found that the "effective control" standard was applied in 33% of 87 cases, and that the relatively low application rate of "effective control" was solely related to the extremely difficult standard of proof. In contrast, the "full control" standard was applied in 80% of the 42 armed conflict cases. Through data comparison, it is evident that the classification of application has practical necessity.

Secondly, by identifying the International Court of Justice's rules for determining transnational harm, relevant data from 34 cases involving environmental damage and nuclear accidents shows that the rule requiring preventive measures accounts for 76.5% of liability determinations. This proportion provides a

reliable basis for applying this rule in the field of cyberattacks. The China National Computer Network Emergency Response Technical Team and Coordination Center monitored 1,455 active command-and-control endpoints used to launch distributed denial-of-service attacks, with 97.1% of these endpoints located outside China. The majority of these endpoints were distributed across the United States (34.2%), the Federal Republic of Germany (18.7%), and the United Kingdom (12.4%). These facts not only vividly illustrate the transnational nature of cyberattacks but also confirm the practical challenges in cyberspace. Specifically, the geographical dispersion of attack sources makes it difficult to determine their origin, and this also poses significant challenges for the attribution of responsibility under rules that require effective state control over specific attack behaviors.

In a quantitative study of 156 major cross-border cyberattacks worldwide between 2015 and 2023, only 12 cases could be clearly confirmed as involving direct state control over the attacks, accounting for 7.7%. In 89 cases, there were instances where states failed to fulfill their duty of care, accounting for 57.1%. This data provides strong support for the supplementary attribution mechanism proposed in this study, known as the “duty of care.” The “scale and effect” standard for the right to self-defense against cyberattacks outlined in the Tallinn Manual 2.0 version exhibits significant subjectivity in practical application. For the same cyberattack incident, the consistency of legal evaluations among different countries based on this standard is only 41.3%, which validates the practical value of the multi-factor comprehensive assessment framework proposed in this study.

The statistical charts of countries' positions in the report reflect that, while the international community generally supports the application of international law to cyberspace, the proportion of countries applying international law to cyberspace has shown a growing trend since 2013. This proportion increased from 62.3% in 2013 to 84.7% in 2021. However, there remain significant divergences regarding the applicable standards. Only 38.2% of countries support the application of preemptive self-defense rights favorable to their own interests in cyberspace, while 71.4% support the application of strict liability standards. Data from the ASEAN Cyberspace Governance Cooperation Empirical Survey Report also effectively illustrates the assessment conclusions regarding the effectiveness of the regional coordination model for ASEAN cyberspace governance. The International Telecommunication Union (ITU) 2020 Global Cybersecurity Index Report noted significant disparities among the ten ASEAN countries, with Singapore leading the pack at 98.52 points and Cambodia trailing at the bottom with 19.12 points. However, the level of cyber governance cooperation among the ten ASEAN countries achieved a 156% increase between 2015 and 2020 through the use of regional coordination mechanisms. This also provides empirical evidence supporting the complementary and mutually beneficial model proposed in this study, which plays a role in narrowing and bridging the gaps and deficiencies in cyber governance capabilities among ASEAN member states. The data on the number of cyberattacks targeting Huawei Group is even more striking. The number of attacks per month increased from around 500,000 to 600,000 in 2013 to over one million per day by 2019, with Huawei Group averaging over one million attacks per day. On average, Huawei faces over 10 cyberattacks per second and is constantly subjected to various cyberattacks. This data clearly demonstrates the fact that the number and intensity of cyberattacks in cyberspace are continuously increasing, providing timely and targeted evidence to support the recommendations proposed in this study for enhancing China's cyberattack governance capabilities.

The aforementioned multi-dimensional and multi-level data not only provides a solid foundation and data support for identifying facts and implementing research conclusions, avoiding theoretical speculation based on insufficient problem awareness, but also ensures that our research is grounded in empirical evidence. Furthermore, it provides material for subsequent more specific data collection and analysis targeting issues, identifying new perspectives on problems, and proposing more targeted and feasible solutions.

3. Research findings on International Law and Cross-Border Cyber Attacks

3.1. Legal Accountability Standards for Cross-border Cyber Attacks

In summary, cross-border targeted attacks in cyberspace have severely undermined the attribution procedures of traditional international law mechanisms for state responsibility. Under the current framework of international rule of law, the “effective control” standard does not align with the technical and comprehensive characteristics of cyberspace, and states cannot prove control over the specific actions of non-state actors through direct control over the attacks. This is because actors in cyberspace can conceal their identities and attack objectives through layered proxy servers, botnets, and other means, and may receive sustained state-sponsored resource support to obtain accurate information targeting specific entities. Therefore, we tend to believe that a state's direct control over a specific cyberattack is not a necessary prerequisite for proving “effective control.” However, the factual standard of “effective

control" remains applicable: for a specific attack where the state lacks provable involvement, the attack must simultaneously possess specific objectives, technical means, objective targets, strategic concepts, and so on. That is, if an attack is carried out with state-sponsored actions or funding, this can serve as the basis for determining "effective control" under the attribution standard. Of course, we believe that, based on this standard, international law should strive to avoid overly stringent factual standards for attribution of responsibility and instead adopt a more appropriate approach that does not consider the active or passive behavior of individual entities during the attack. As long as a state engages in an overall offensive plan or provides funding for specific control, it can be held accountable, thereby developing the applicable rules for the "comprehensive control" standard. The "comprehensive control" standard should be applicable in cyberattacks within the context of traditional armed conflicts. This particularly refers to transnational, purposeful attacks that may cause substantial harm to the target entity (such as casualties or destruction of property) or severe environmental damage (such as the destruction of critical infrastructure). The "comprehensive control" standard is closely aligned with the intentional causing of death or bodily harm, or other states or harmful consequences.

Liability should be commensurate with risk tolerance. In cases involving transnational interests being harmed, the duty of care rule supplements the general liability principle, applying when it cannot be proven that a state directly controlled the cyberattack. This rule requires states to take reasonable measures to prevent their territorial or jurisdictional cyber infrastructure from being used to attack other networks, such as through necessary cybersecurity administrative measures, timely responses to cyberattacks, and necessary information sharing and cooperation with other states. If a state fails to fulfill its reasonable preventive obligations, thereby allowing its network resources to be maliciously exploited by others to cause harm to another state, it may still be held liable for violating its duty of care, even if it cannot be proven that the state directly participated in or controlled the cyberattack occurring within its territory. We have found that in cases involving "jump-off" technology during cyberattacks, applying this rule to prevent indirect attacks utilizing another state's network infrastructure may be particularly effective. The reasonable allocation of the burden of proof is a crucial aspect of applying liability criteria. We propose adhering to the basic principle of "he who asserts must prove," while applying special rules for the reasonable allocation of the burden of proof based on different circumstances. The victim state must provide evidence to prove the existence of the attack, the damage caused by the attack, and a reasonable connection between the attack and a specific state. The accused state must provide relevant materials to assist in verifying the facts, especially if it possesses certain unique information resources. The reasonable allocation of the burden of proof safeguards national sovereignty while ensuring the fairness and effectiveness of the attribution process, establishing a credible cyberattack attribution system that lays the foundation for an effective attribution procedure. By categorizing and applying the two accountability standards of "effective control" and "full control," along with the supplementary standard of due diligence, a multi-dimensional accountability standard system has been established. This not only fills the theoretical gap in existing international law regarding the resolution of cyberattack accountability issues but also effectively addresses the practical challenges faced in accountability determinations.

3.2. Standards for the Application of Self-Defense in Cyber Attacks

Whether the right to self-defense applies to cyberattacks is the greatest challenge currently facing international law, and this challenge becomes even more complex when traditional rules of self-defense are applied to cyberspace. The system of self-defense established under Article 51 of the United Nations Charter was originally designed to address armed attacks in the physical realm, and applying it to the virtual cyberspace requires rethinking and redefining, which is a highly challenging conceptual restructuring process. The "Tallinn Manual 2.0 on the Application of International Law in Cyberspace," currently the most authoritative and widely influential research document on the application of international law in cyberspace, clearly states that determining whether a cyber-related action constitutes the "use of force" should be based on factors such as "scale" and "effect," rather than on 'technical' or "methodological" aspects of the action. While this results-based approach has logical merit, it is indeed challenging to make precise judgments in the highly uncertain field of cyberspace security, especially when the consequences of a cyberattack have not fully manifested but a judgment must still be made. In this regard, I believe that the applicability of the right to self-defense under cyberattacks should not be limited to single factors such as "scale and effect," but rather a set of criteria composed of multiple factors should be established.

This model should not only consider the objective actual damage caused by the cyberattack but also take into account the nature of the attack target, the persistence and systematic nature of the attack, and the strategic objectives of the attacker. The importance of preemptive self-defense in cyberattack defense is largely theoretical. While countries like France and Australia have affirmed the legality of preemptive

self-defense in their national policy documents, such statements, if lacking strict limitations, could easily be abused. Looking back at the conditions for the application of preemptive self-defense established in the "Caroline Incident" in the international community—such as "necessity, urgency, the necessity of having no other means available, and no time for careful consideration"—these strict application standards should be interpreted and applied even more strictly in cyberspace. Given the covert nature of cyberattacks (such as advanced persistent threats that can remain undetected in a system for months), their sudden onset (from initiation to causing actual damage may take only seconds), and the difficulty in attributing responsibility, I believe that the application of the right to preemptive self-defense in response to cyberattacks should be subject to strict limitations. The criteria for determining that an attack is imminent must be strictly defined, meaning that there must be evidence from professional institutions based on sufficient computer technical evidence proving that the preparatory work for the attack has been largely completed and that it has the capability to be launched immediately. Preemptive defensive measures must strictly adhere to the principles of necessity and proportionality, and defensive actions must not exceed the reasonable limits necessary to prevent a specific attack. States exercising preemptive self-defense should also bear a higher burden of proof than under normal circumstances, providing sufficient evidence to demonstrate the existence of an imminent cyberattack threat, to prevent the right of self-defense from being abused as a pretext for aggression.

The reasonable selection of the target of self-defense not only involves issues of international law theory but also directly impacts the feasibility and legality of countermeasures against cyberattacks in practice. The Tallinn Manual 2.0 version asserts that states possess the right to self-defense against cyber activities conducted by terrorist organizations without state support that reach the severity of armed attacks. While this may have some rationality from the perspective of addressing non-traditional security threats, it has sparked significant academic debate in the international academic community. From the perspective of the relationship between the justifications of international law and international practice, the author believes that expanding the scope of self-defense to non-state actors cannot be supported. Cyberattacks launched by non-state actors can be addressed and regulated through other normative methods, such as further improving international criminal judicial assistance or enhancing mutual attention among states, rather than simply expanding the scope of self-defense, which could lead to an imbalance in the international order. The exercise of the right to self-defense in cyberattacks is subject to the principles of necessity and proportionality. These two traditional principles of international law take on special meanings and implications in the context of cyberattacks. Necessity refers to the fact that the self-defense measures taken are the only possible response to the cyberattack, and there are no effective technical defensive measures, diplomatic channels, or international cooperation measures available to halt or mitigate the attack. Proportionality means that the scale, intensity, and form of self-defense actions should be commensurate with the scale or severity of the original attack, and should not transform self-defense into retaliation or punishment. Cyberattacks typically exhibit characteristics such as concealment and cascading effects, making it difficult to accurately assess the full extent of potential losses during the initial stages of an attack. As a result, determining the proportionality of self-defense responses becomes more complex and challenging.

It is necessary to establish a set of standards for assessing the damage caused by cyberattacks, comprehensively analyzing factors such as the scale of data destruction, the duration of system paralysis, the technical or financial costs required for restoration, and the potential secondary social disasters that may be triggered. This would provide a relatively "neutral and objective" reference standard for exercising the right to self-defense. Technical attribution issues remain the most direct practical bottleneck in determining the exercise of self-defense rights in the field of cybersecurity. During actual attack incidents, technical tracing of attack sources is difficult to determine due to technical obstacles such as IP address tampering, the use of botnets, and the deliberate masking of attack routes. In response to the widespread uncertainty in technical attribution, it is recommended to establish different levels of trigger conditions for addressing such challenges.

For cyberattacks with sufficient evidence pointing to their origin, traditional self-defense rights may be applied. For cases where there is reasonable suspicion but insufficient evidence to confirm a cyberattack, diplomatic means and international cooperation should be prioritized to resolve the issue before escalation to war. For cyberattacks where attribution remains impossible to determine, the focus should be on enhancing defensive cyber capabilities rather than hastily resorting to retaliatory self-defense. Such a tiered approach fully respects the foundational principles of traditional self-defense while also accounting for the unique circumstances arising from the technical difficulties of attribution, which can lead to uncertainty regarding the identity of actors in cyberspace. It does not seek to radically transform the existing legal framework for the application of self-defense but instead balances adherence to fundamental principles with consideration for the technical challenges involved. The pursuit and protection of a nation's legitimate rights and interests in cyberspace should not, due to the improper

exercise of the right to self-defense, evolve into a strategic struggle that negates the primary rights of a nation in the field of cybersecurity in the digital age. Through a multi-faceted, multi-standard framework for judgment, strict conditions should be imposed on preemptive self-defense, its scope of application should be limited, and a layered response strategy should be established, among other rule frameworks.

3.3. Complementary and Progressive Model for the Application of International Law in Cyberspace

The application of international law to cyberspace has become a central focus of contemporary international legal research. The high frequency of cross-border cyberattacks, the rapid development of network technology, and the rapidly changing international political environment have compelled the international community to establish a legal framework that effectively regulates cyber threats while balancing the interests of all nations. The mainstream interpretive approaches—the instrumentalist theory, the customary international law theory, and the alternative methodology—each have their obvious limitations. The instrumentalist theory equates cyberspace with the physical world, the customary international law theory faces the challenge of an overly lengthy codification process, and the alternative methodology risks fragmentation.

Given this, we believe that the core of the legitimacy of international law's application in cyberspace lies in the continuity of its social foundation. Despite cyberspace's unique attributes (such as virtuality, transnationality, and technological dependency), it remains an integral part of human social activities, with states as the primary actors and rule-makers in cyberspace activities. The complementary and progressive model is a theoretical framework we propose to address the structural challenges of applying international law in cyberspace. This core theoretical framework is grounded in the dual foundations of cyberspace's technological attributes and state sovereignty, achieving multi-layered, dynamic application of international law through the two core mechanisms of “complementarity” and “progressiveness.” “Complementarity” refers to both acknowledging and applying existing international law rules (such as continuing to apply traditional international law principles in cyberspace, including the principle of sovereign equality, the principle of non-interference in internal affairs, and the principle of non-use of force or threat of force) while also recognizing the necessity of new rules tailored to the characteristics of cyberspace. The term ‘co-progression’ refers to the gradual and multi-layered nature of rule development, advocating the use of ‘soft law mechanisms,’ 'regional rule experiments,‘ and 'multi-center governance models’ to expand the application of international law in cyberspace." For example, the ASEAN cyber governance cooperation model provides the necessary conditions to bridge differences and strengthen regional identity. ASEAN should also fully leverage its regional leadership role (while maintaining necessary caution toward external major powers such as the United States), thereby forming a governance-oriented approach that embraces an open attitude toward the participation of all stakeholders. A coordination model characterized by “top-down” and “bottom-up” interactive, mutually beneficial coordination—where appropriate positive responses are made to regional institutional demands while selectively implementing and enforcing corresponding rights and obligations—can serve as a reference for the application of the aforementioned complementary and progressive model.

The collaborative and progressive model advocates “tiered application” in terms of rules, with the application of international law in cyberspace limited to three tiers: principle application, rule interpretation, and rule creation. Each issue in cyber governance corresponds to different tiers of international law rules. In terms of governance entities, the model advocates “multi-stakeholder governance,” which centers on states while incorporating intergovernmental organizations, non-governmental organizations, technical communities, and the private sector to enhance the diversity and pluralism of governance entities. In terms of the procedures of cyber governance, the model advocates “coordinated advancement,” which involves promoting the application and evolution of international law in cyberspace through a three-step approach of soft law, regional trials, and global coordination, while balancing different value orientations such as security and freedom, development and governance, and sovereignty and cooperation. In terms of the values of cyber governance, the model advocates “balanced coordination.”

The complementary and progressive model embodies a high degree of strategic and practical unity, helping to shape a common understanding of the application of United Nations-led international law in cyberspace at the global level, assisting regional organizations in developing regional cyber governance rules at the regional level, helping countries internalize international law rules into domestic law rules at the national level, and coordinating legal rules and technical standards rules at the technical level. In the field of regulating cross-border cyberattacks, the complementary and progressive model demonstrates unique regulatory advantages. By leveraging the principle of the prohibition of the use of force, the duty of care rule, and international cooperation mechanisms to jointly regulate cross-border cyberattacks, it

establishes a targeted, multi-tiered regulatory framework. This framework can regulate both state-sponsored high-intensity cyberattacks and persistent low-intensity cyberattacks by non-state actors.

Additionally, a “technical-legal” dual evidence rule has been established, where the presumption of technical attribution and the presumption of legal liability complement each other to address the challenges posed by the difficulty of attributing cyberattacks to legal application. The supplementary development model innovatively combines the two foundational concepts of rule supplementation and legal development, providing a framework for the application of international law in cyberspace that balances theoretical considerations with practical insights. It respects the characteristics of cyberspace and the sovereignty of states while also emphasizing the universality and global nature of cyberspace governance. It can address current governance challenges through the positive interaction between the application of international law in cyberspace and the development of cyber technology, while also leaving room for flexibility and institutional development in the future evolution of international rules governing cyberspace.

3.4. China's Approach to Cyberattack Governance

China faces dual pressures in the governance of cyberattacks, as both the largest developing country and a major cyberpower, it must not only ensure its own cybersecurity but also contribute to the governance of cyberspace. According to monitoring by the China National Computer Network Emergency Response Technical Team/Coordination Center, the severe situation of cyberattacks in China is characterized by centralized attack sources, complex attack methods, and precise attack targets. For example, cyberattacks targeting Huawei Group surged from 500,000 to 600,000 per month in 2013 to over one million per day in 2019. This indicates, on the one hand, the severe security situation facing China's high-tech enterprises, and on the other hand, the urgency of constructing a comprehensive cyber governance framework. In this context, China has proposed the concept of building a “community with a shared future in cyberspace,” based on a rational perspective that transcends traditional zero-sum games and a sense of responsibility to construct a new order in cyberspace based on interdependent interests. This aims to transcend zero-sum game thinking, becoming a Chinese wisdom for governing the global cyberspace order and a Chinese solution to address the fragmentation of cyberspace governance. China faces two main dimensions of challenges in cyberattack governance. The first is the domestic legal system dimension, which urgently requires accelerating the legislation of the Cybersecurity Law. For example, defining cross-border cyberattacks, establishing legal accountability for such attacks, and imposing corresponding penalties. The second is the international cooperation dimension, which involves actively promoting the formulation of the International Code of Conduct for Cyberspace and advocating these cyber governance concepts through platforms such as the Shanghai Cooperation Organization and the BRICS countries. China should promote cybersecurity cooperation with other countries and establish cybersecurity cooperation between countries and industries with countries along the Belt and Road Initiative. Third, on the technical and capability level, China should improve the research and development of cyberattack attribution technology and establish corresponding laboratories. Specifically, it should establish a national-level cyberattack attribution laboratory to provide technical support for legal accountability in the field of cyberattacks.

China's practice of cyber attack governance advocates "offense as defense and joint governance", and achieves a three-dimensional governance structure by creating multi-level defense, establishing a coordination and linkage mechanism, and strengthening international police cooperation. In terms of building a defense system, China should create a real-time early warning and prevention and control system covering critical information infrastructure, improve the classified cybersecurity protection system, and strengthen protection in key areas such as finance, energy, and transportation. In terms of the coordination and linkage mechanism, the Cyberspace Administration of China (CAC) will take the lead in establishing a coordination mechanism for responding to cyber attacks, and coordinate the prevention, response, and handling of cyberattacks. In terms of international cooperation, China should strengthen dialogue and cooperation with important countries and promote the signing and implementation of treaties on extradition for cybercrimes. In terms of improving China's discourse on the legal governance of cyber attacks, China should adopt three paths: constructing theories, formulating rules, and demonstrating solutions. "Constructing theory" refers to China's theoretical system of cyberspace international law with Chinese characteristics based on China's practice, and putting forward representative and influential arguments on issues such as cyber sovereignty and data sovereignty. "Rule-making" means actively participating in the rule-making work of cyber governance within the framework of the United Nations, the International Telecommunication Union, etc., promoting China's concept of a "community with a shared future in cyberspace" to be confirmed in international normative documents, and "giving voice to China" when revising academic texts such as the Tallinn Manual. The "model plan" is to demonstrate the effectiveness of China's plan with successful practice plans.

China's cyberattack governance scheme can serve as a model for developing countries, advocating a balance between cyber sovereignty and international cooperation, maintaining a balance between cybersecurity and development in cyberspace, and balancing technology and rules. It not only safeguards China's cybersecurity interests but also contributes to establishing a fair and reasonable international order in cyberspace. In the era of globalization, China should adopt an inclusive and open attitude, actively fulfill its international obligations while protecting its own cybersecurity, and propose practical solutions and constructive suggestions. It should enhance its ability to set the agenda and exert influence in the field of international cybersecurity law, making greater efforts to promote the development and maturation of international cybersecurity law.

4. Conclusion and Outlook

4.1. Research Conclusions

In the future, global cyberspace security will become a major risk and challenge affecting areas such as global political and economic security. Cross-border cyberattacks have already emerged as a challenge and disruption to the traditional legal order and rules of international law. This article explores the basic applicability of international law in regulating and addressing cyberattack behaviors, as well as issues related to attribution of responsibility, the right to self-defense, and specific institutional pathways, aiming to reveal the tension between legal logic and real-world conflicts. It is evident that the international legal system has legal sources that are generally applicable, but in specific responses, it faces challenges such as legal systems and rules being overly outdated, unclear attribution of responsibility, and insufficient sanctions. Beyond state responsibility, solutions involving the effectiveness of actors will increasingly come to the fore. Therefore, using the criterion of “effective + willing” to determine effectiveness, we should establish evaluation standards for whether cyberattacks constitute “armed attacks” and reconstruct and set new benchmarks for assessing responsibility for cyberattacks. It is proposed to establish a cyber governance system and mechanisms that combine a functional attribution of responsibility framework with the realization of multilateralism, alongside a cyber legal system implemented through soft law. This should be achieved by promoting the establishment of unified technical standards, enhancing international tracking capabilities, and establishing mechanisms for capacity-building, thereby mitigating the asymmetry of national capabilities in global cyberspace security to some extent.

In summary, the international community should regulate cross-border cyberattacks by respecting traditional legal principles while appropriately addressing new digital challenges, establishing a rule system that is both legitimate and operational. This should be a universal and important issue for the international community to address in the future.

4.2. Future Outlook

The author has conducted research on the theoretical issues of international regulation of cross-border cyberattacks. While some theoretical breakthroughs have been achieved, the research methods and conditions still have certain limitations and require further study.

(1) This paper employs literature analysis and case study methods to organize and construct relevant theories, which provides a solid theoretical foundation for the study. However, the lack of large-scale empirical data limits the general applicability of the research conclusions.

(2) The self-defense standards constructed in this paper are theoretically comprehensive, but their ability to flexibly respond to evolving cyberattack technologies and threat scenarios remains to be tested over time.

For future research, the first priority is to further deepen and innovate empirical research. Given the practical needs of the development of international law in cyberspace, constructing a case database for cyberspace and utilizing methods such as questionnaire surveys and expert interviews can provide more data support for China's research on international law in cyberspace. For example, collaboration with companies in the cybersecurity field, government agencies, and international organizations could be considered to obtain more detailed reports on cyberattacks, assessments of damage outcomes, and evaluations of response effectiveness. This would help validate and assess the rationality and practical effectiveness of the attribution standards and self-defense application standards proposed in this paper in specific practices. Additionally, to better conduct in-depth empirical analysis, case studies of international cyber law could be conducted. Selecting several representative cases of international cyber law for analysis could provide more concrete ideas and directions for the application of international cyber law. Through further comparative research, ideas and methods can be provided to facilitate the convergence and cooperation of international cyber law rules among countries and address the shortcomings of international governance. Additionally, by expanding the scope of research subjects,

studies on international cyber law in specific regions (primarily China and its neighboring countries and regions) can be conducted to better understand the development and changes of international cyber law in different regions. This will provide institutional frameworks for international governance and promote the transition of the international order from fragmented governance to institutionalization and mechanization. In addition, based on the latest developments in cyberspace technology, in the process of the development and application of big data, cloud computing, artificial intelligence, quantum computing, and blockchain, in the intersection of information technology and international law in cyberspace, how the technical and legal systems of international law in cyberspace are constituted and transformed is an important theoretical issue and research path for further enriching and developing international law in cyberspace in the future. At the level of international cooperation mechanisms, the trend toward the globalization of cyberattacks is becoming increasingly evident, and the roles of multi-level governance platforms such as the United Nations, the International Telecommunication Union, and regional organizations are growing more prominent. Analysis of international cooperation mechanisms should also become an important focus of future research, with efforts directed toward identifying the shortcomings of current international cooperation mechanisms and proposing directions for improvement.

References

1. Masera, R. (2023). Web 1.0, 2.0, 3.0; InfoSphere; Metaverse: An Overview. Monetary, Financial, Societal and Geopolitical Transformation Cusps. *Monetary, Financial, Societal and Geopolitical Transformation Cusps (January 14, 2023)*.
2. Luidmila, T. (2021). The issue of state sovereignty in cyberspace. *Legal Issues in the digital Age*, (2), 49-67.
3. Tsaugourias, N. (2017). Law, borders and the territorialisation of cyberspace. *Indonesian J. Int'l L.*, 15, 523.
4. Faga, H. P. (2017). The implications of transnational cyber threats in international humanitarian law: analysing the distinction between cybercrime, cyber attack, and cyber warfare in the 21st century. *Baltic JL & Pol.*, 10, 1.
5. Naseeb, J., & Tariq, A. (2024). Impact of cyber-attacks on national security and international relations. *International Journal for Conventional and Non-Conventional Warfare*, 1(1), 86-96.
6. Stevens, T. (2017). Cyberweapons: an emerging global governance architecture. *Palgrave Communications*, 3(1), 1-6.
7. Bjorge, E. (2023). General Principles of Law Formed Within the International Legal System. *International & Comparative Law Quarterly*, 72(4), 845-867.
8. Banks, W. (2021). Cyber attribution and state responsibility. *International law studies*, 97(1), 43.
9. Donald, D. C. (2020). Legal System Network Effects and Global Legal Development. *Notre Dame J. Int'l Comp. L.*, 10, 267.
10. Adonis, A. A. (2020). International law on cyber security in the age of digital sovereignty. *E-International Relations*, 14, 1-5.
11. Hines, B. (2024). Reinterpreting the legality of forcible self-defence in response to non-kinetic cyber attacks. *Melbourne Journal of International Law*, 25(1), 51-94.
12. Dutchak, S., Opolska, N., Shchokin, R., Durman, O., & Shevtsiv, M. (2020). International aspects of legal regulation of information relations in the global internet network. *J. Legal Ethical & Regul. Isses*, 23, 1.
13. Hayward, R. J. (2017). Evaluating the Imminence of a Cyber Attack for Purposes of Anticipatory Self-Defense. *Colum. L. Rev.*, 117, 399.
14. He, X. (2023). The Impact of Russia-Ukraine Cyberwarfare on the Application of the Right to Self-Defense in Cyberspace and Implications. *US-China L. Rev.*, 20, 113.
15. Oorsprong, F., Ducheine, P., & Pijpers, P. (2023). Cyber-attacks and the right of self-defense: a case study of the Netherlands. *Policy Design and Practice*, 6(2), 217-239.
16. Alkharman, J. A., Drawsheh, S. A. A., Al-Khataybeh, M. M., BaniYounes, Z. B., Hamid Darawsheh, N. A., & Alrashdan, H. (2024). Cyber Attacks and its Implication to National Security: The Need for International Law Enforcement. *Pakistan Journal of Criminology*, 16(3).
17. Katagiri, N. (2021). Why international law and norms do little in preventing non-state cyber attacks. *Journal of Cybersecurity*, 7(1), tyab009.
18. Mačák, K. (2017). From cyber norms to cyber rules: re-engaging states as law-makers. *Leiden Journal of International Law*, 30(4), 877-899.
19. Haataja, S. (2022). Cyber operations against critical infrastructure under norms of responsible state behaviour and international law. *International Journal of Law and Information Technology*, 30(4), 423-443.
20. Finnemore, M., & Hollis, D. B. (2020). Beyond naming and shaming: Accusations and international law in cybersecurity. *European Journal of International Law*, 31(3), 969-1003.
21. Reichler, P. S., & Parkhomenko, Y. B. (2018). Nicaragua v. United States and Matters of Evidence Before the International Court of Justice. *Nicaragua Before the International Court of Justice: Impacts on International Law*, 43-56.
22. Strapatsas, N. (2017). The international criminal judgments: from Nuremberg to Tadić to Taylor. In *Research Handbook on International Courts and Tribunals* (pp. 79-121). *Edward Elgar Publishing*.
23. Haider, A., Iqbal, S., & Zeb, B. (2024). The Corfu Channel Case and the Limits of Self-Defense. *Journal of Islamic and Social Studies*, 1-9.

24. Tladi, D. (2017). The principles of sustainable development in the case concerning Pulp Mills on the River Uruguay. In *Sustainable Development Principles in the Decisions of International Courts and Tribunals* (pp. 242-254). *Routledge.*
25. Putra, J. I. S., Sefriani, S., Febriani, Y., Khoirunnisa, H., & Ramadhan, M. R. (2024). Self-Defense Justifications: from Caroline Case to Russia v Ukraine. *PADJADJARAN JURNAL ILMU HUKUM (JOURNAL OF LAW)*, 11(3), 365-384.
26. Whitt, S., Shkliarov, V., & Mironova, V. (2025). Going public about cyber attacks: public threat sensitivity and support for escalation in the United States and Russia. *Journal of Cybersecurity*, 11(1), tyaf007.
27. Chen, X., & Yang, Y. (2022). Different shades of norms: Comparing the approaches of the EU and ASEAN to cyber governance. *The International Spectator*, 57(3), 48-65.