International Journal of Law, Policy & Society

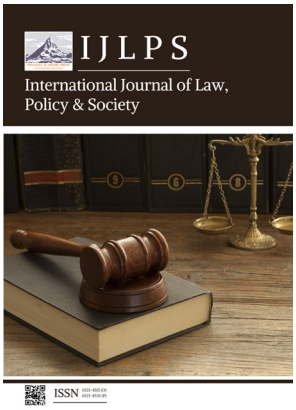
Vol. 1 No. 1 2025

Article **Open Access**

Non-Zero-Sum Game Analysis the Controversy of Cyber Attacks Constitutes the Use of Force

Yuchen Han [1,*]

[1] The University of New South Wales, Sydney, New South Wales, Australia
* Correspondence: Yuchen Han, The University of New South Wales, Sydney, New South Wales, Australia



Received: 04 May 2025
Revised: 18 May 2025
Accepted: 09 June 2025
Published: 14 June 2025

Abstract: This paper examines the evolving challenges of cyberattacks within the framework of international law, highlighting the inadequacy of traditional legal doctrines in addressing the complex dynamics of cyberspace governance. It analyzes the divergence between dominant international camps advocating either "Internet Freedom" or "Cyber Sovereignty", and the resulting zero-sum competition that hinders cooperative security efforts. Through case studies such as the NotPetya and Stuxnet attacks, the study underscores the limitations of existing legal instruments like the Tallinn Manual and explores the necessity of refining legal standards and attribution mechanisms. The paper further advocates for a shift from a zero-sum logic to a non-zero-sum model emphasizing institutional innovation, mutual trust-building, and integrated defense strategies. Practical recommendations include enhancing critical infrastructure defenses and establishing international confidence-building measures to foster sustainable cooperation in cyberspace governance.

Keywords: cybersecurity; international law; Cyber Sovereignty; Internet Freedom; zero-sum game

1. Introduction

1.1. Research Background

Since the Charter of the United Nations (UN Charter) was established earlier than the digital age, it exhibits hysteretic nature. With the emergence of the information network era, cyber attacks have increasingly posed a threat to national security. However, the identification of "Use of Force" in international law is also facing significant challenges. UN Charter Article 2 (4) forbids the use of any form of force against another country's sovereignty and territorial integrity. Nevertheless, the covert and transnational nature of cyber attacks breaks through conventional concepts, triggering legal disputes regarding whether such actions constitute the "Use of Force".

1.2. Research Issues and Significance

Discuss the principles that delineate the nature of force in cyber attacks and explore potential cooperation mechanisms. Theoretically, clarifying the compatibility of cyber attacks with the concept of "Use of Force" under the framework of international law helps facilitate the dynamic evolution of international legal norms. At the practical level, this clarification provides a feasible basis for building a cooperation mechanism aimed at enhancing security governance in cyber attacks [1].

1.3. Research Methods

This paper employs a case analysis approach, utilizing the Stuxnet virus and NotPetya attack as samples, alongside a literature review method, combined with a critical analysis of Tallinn Manual 2.0 and international law texts to investigate the legal dilemma surrounding the characterization of force in cyber attacks and the potential solutions.

2. Cyberattacks May Constitute a Source and a Flexible Interpretation of the Use of Force

UN Charter art. 2 (4) prohibits all forms of force or coercion against the political independence as well as the territorial integrity of other countries. Traditionally, the term "Use of Force" mainly refers to military actions; however, international law does not exclude the applicability of non-military means. Consequently, if a cyber attack infringes upon sovereignty at its core, it may be classified as a non-traditional armed attack. This perspective somewhat broadens the traditional understanding of force and underscores the primacy of sovereignty within international law [2].

Tallinn Manual 2.0 further refines the criteria for cyber attacks, suggesting that if the damage to physical facilities results in casualties and is almost equivalent to traditional force, it can pose a "Use of Force" and may trigger the right to self-defense under Article 51 of the UN Charter.

Both sets of standards broaden the definition of the "Use of Force" in the context of cyber attacks, although there are notable differences between them. To be specific, the international law framework is more focused on sovereignty, whereas the Tallinn Manual concentrates on the threshold for physical consequences. The intersection of these two perspectives lies in whether the executed cyberattacks significantly undermine or affect a state's capacity to exercise its sovereignty [3]. Additionally, this consideration has led to the notion that under certain conditions, cyber attacks might be identified as a source of use of force within international law. This development is opening up new forms of attack and novel methods for legal interpretation and classification.

3. Cyber Attacks as "Use of Force" International Law Disputes

3.1. Traditional "Use of Force" Criteria: Physical Consequences Priority Principle

The UN Charter, Article 2 (4), prohibits countries from using or threatening to use force against other states. However, the definition of "Use of Force" is primarily assessed based on the physical consequences it produces, such as casualties and property damage resulting from military operations. It is not difficult to see that traditional definitional criteria have led to a long-standing fixed mindset. Nevertheless, with the advent of the digital age, the applicability of this interpretation in cyberspace security has become contentious [4].

Taking the case of Nicaragua as an example, the International Court of Justice (ICJ) emphasized that the right to self-defense, as articulated in UN Charter Article 51, would only be invoked if an incident reached a level equivalent to "Conventional Force". The understanding of this also obviously implies the physical threshold; This standard constitutes a heavy reliance on physical consequences, and thus inadequately reflects the particularity and permeability of cyberspace security, where attacks on critical infrastructure such as power grids may paralyze essential systems and result in significant real-world damage.

The Tallinn Manual 2.0 attempts to address these disputes by asserting that a cyberattack poses a "Use of Force" if this action directly leads to physical damage or loss of life. However, the manual still fails to adequately define non-physical consequences, leaving a significant gap in the legal framework for cyber conflict [5]. To some extent, this stance contradicts notions within international law suggesting that significant economic disruption and interference with essential infrastructure may also qualify as uses of force.

Moreover, when actions involve interference in another country's internal affairs through cyber means to potentially affect the sovereignty of other countries, it becomes challenging to ascertain whether such actions could influence another nation's political independence under UN Charter interpretations. What remains clear is that experts on the international panel are beginning to acknowledge these complexities.

3.2. Particularity of Cyber Attack Forms

Cyber attacks often have multiple technical characteristics different from traditional forces: first, it is highly concealed. For example, APT attacks often use techniques such as code obfuscation to remain hidden in target systems for extended periods, making them difficult to detect or respond to effectively in a short time. The second is transnational, where attackers are adept at using international servers anonymously across multiple jurisdictions. In addition, there is a significant asymmetry, the use of low-cost network tools to carry out devastating damage to key high-value targets, attack benefits and defense costs are unbalanced [6]. In the case of Stuxnet, a targeted attack may trigger a chain reaction due to system interconnectivity, causing uncontrollable cascading effects across digital infrastructure and leading to unforeseen damage. These characteristics suggest that current cyber attacks may escalate from incremental threats to systemic risks, triggering qualitative changes. The existing international legal framework struggles to provide effective defense, highlighting the urgent need for a dynamic and adaptive cybersecurity defense system [7].

3.3. The Lag of the Original Framework of International Law

Nowadays, international law exhibits a notable lag in addressing cyberattacks. The primary challenges revolve around the dilemma of attribution and the ambiguity surrounding the threshold for assessing consequences.

3.3.1. Challenges in Attribution and State Responsibility

Each country encounters a variety of cyber threats from diverse actors, including hacker groups, terrorists, and even state entities. Consequently, nations must first determine whether cyber attacks should be classified as general law enforcement issues or national security concerns. Attribution primarily refers to identifying the responsible party behind a cyber attack. One significant challenge in this regard arises from Article 2(4), which pertains exclusively to cyber actions conducted by or attributable to states. It is evident that the criteria for determining a violation of this article remain ambiguous and unresolved [8].

Simultaneously, there are pressing questions regarding how to confirm whether the cyber attack actors belong to state organizations and whether there is clear proof to demonstrate the specific intent of the attacking nation. This issue becomes particularly complex in cases involving cross-border cyber attacks that target non-state actors, such as hacker organizations, or employ technical disguises; these scenarios frequently involve state actors without direct attribution.

3.3.2. Consequences Assessment of Inertia and Force Threshold Dispute

The Tallinn CyberWarfare Manual states that a cyberattack must be comparable in scale to a non-cyber operation involving the use of force in order to qualify as such under international law. However, due to the particularity of the network attack itself, there are still many problems in determining the start time and whether the behavior itself can invoke the definition of self-defense.

To date, prevailing scholarly opinion holds that Article 69 of the Tallinn Manual 2.0 requires demonstrable damage to persons or property for an action to be classified as a use of force. As you can see, scholars are trying to refine the criteria [9]. However, current definitional standards predominantly emphasize physical assessments of consequences.

This focus is rooted in a longstanding tradition of conceptualizing the use of force within conventional frameworks. Consequently, this reliance on traditional metrics introduces considerable ambiguity into the definition itself:

1) Disputes over Non-physical Consequences:

Particularly concerning whether the threshold for serious economic loss resulting from a cyber attack is met. In the case of Stuxnet, the incident had a direct impact on Iran's economy, leading to substantial economic losses due to international sanctions and instilling a profound sense of insecurity within society. However, it has not been classified as an act of force because its direct effects on individuals and societal structures were minimal. This raises questions about whether the current threshold for defining cyber attacks as uses of force is set too high [9]. Moreover, the ambiguity surrounding this threshold may contribute to an expanded legal gray area, complicating international legal responses.

2) Lack of Quantification:

While certain forms of economic coercion may fall short of the threshold for a "Use of Force", cyber activities that cause significant economic harm could nonetheless be viewed as such under international law. However, in the process of this presumption, there is a lack of clear criteria. For instance, a catastrophic cyber attack on a nation's stock market might be deemed a use of force; however, the term "Catastrophic" is contingent upon quantifiable metrics such as financial loss and property damage. The lack of an established quantitative standard complicates practical assessments and applications in this context.

4. Legal Dispute Analysis of Typical Cases

4.1. Stuxnet Controversy

The Stuxnet virus, disclosed in 2010, is considered a landmark cyber incident that provides critical insights into the classification of cyber operations and the development of future cybersecurity defense strategies. The virus was specifically engineered to damage centrifuges at Iran's nuclear facilities, with the intent of halting or delaying Iran's nuclear program. Some experts argue that both the available evidence and strategic motives point to the United States and Israel as likely actors behind the attack. However, thus far, there has been an absence of a definitive evidence chain to confirm these suspicions, and neither country has publicly acknowledged any responsibility for the incident [10,11]. This case also highlights the significant challenges in applying international legal rules to questions of attribution. To date, there remains considerable controversy over whether the incident constitutes a "Use of Force" under international law:

1) Support constitutes Use of force:

Under the eight-element principle, including seriousness, immediacy, and invasions, the physical effects of stuxnet and the loss of centrifuge function are close to traditional military actions, which is consistent with the prohibition of the "Use of Force" under Article 2 (4).

2) Objection to the Use of Force:

The assessment of whether the operation constitutes a use of force should be conducted within the framework of international law governing the use of force, rather than international humanitarian law, which applies once an armed conflict is underway. Given that this cyber operation does not have a direct impact on civilians or society, it can be classified as non-lethal. Considering the principle of proportionality, there are no casualties and clear implementation subjects. Furthermore, when considering the principle of distinction, it is challenging to obtain clear evidence demonstrating a military objective for this operation. While some experts argue that the creator of the virus possesses significant knowledge about facilities in Iran and suggest that its motive is to impede Iran's nuclear program, definitive proof remains elusive. Consequently, it is difficult to categorize this action as constituting a "Use of Force".

4.2. NotPetya Attack

The NotPetya campaign commenced in June 2017, strategically timed to coincide with a significant holiday in Ukraine [12]. The malware was disguised as ransomware and propagated through financial and tax infrastructure, causing widespread disruption to global enterprises and resulting in substantial economic losses. Several governments, including Australia, the United States, and the United Kingdom, have publicly attributed the attack to Russian military actors, although Russia has denied these allegations and no definitive international attribution has been established. Whether the incident constituted a "Use of Force" remains a matter of debate:

1) Supporting the characterization of "Force":

Scholars believe that the attack violates sovereignty, mainly in the form of an invisible violation of territorial integrity by causing an attack on the network infrastructure that leads to long-term unusability. This perspective posits that cyberspace should be regarded as an extension of national territory. Concurrently, this action is accompanied by coercive measures directed at Ukraine, aimed at disrupting the economic order and impacting societal stability; these actions may be interpreted as a violation of the principle of non-interference to some extent. Collectively, these elements could be categorized as unauthorized use of force.

2) Against the characterization of "Force":

In the realm of cyberspace security, attribution necessitates both clear technical evidence and reliable sources of information. We have only seen technical information and indications that the attack may have originated in Russia; It should be acknowledged that due to the inherent anonymity and transnational structure of the Internet, collecting definitive attribution evidence remains a significant technical and legal challenge. Therefore, some scholars also doubt that anonymous network operations are difficult to apply the original traditional force standards.

4.3. Unilateral Actions in Cyberspace and Dilemmas of International Law: Reflections on Stuxnet and Notpetya Attacks

Cyberspace is often portrayed as a binary domain of winners and losers, but international relations in the real world are rarely so clear-cut. And the militarization of cyberspace is challenging traditional models of international law.

Firstly, the prevalence of unilateral actions leading to the escalation of retaliation is noteworthy. Stuxnet is frequently cited as a quintessential example of non-traditional or asymmetric warfare in cyberspace. However, it simultaneously reinforces unilateralism by circumventing the traditional mechanisms of force established by international law, thereby inevitably heightening the risk of exacerbating zero-sum dynamics. Currently, international law continues to define force primarily through "Physical Consequences", which can easily precipitate an escalation in mutual retaliatory measures. A notable example is that Iran's advancement in cyber warfare capabilities following Stuxnet has contributed to such security dilemmas [13].

In addition, the dilemma arising from the legal gray area: The NotPetya attack resulted in significant economic losses globally, yet the United Kingdom, the United States, and Australia responded solely with unilateral condemnations through diplomatic channels without activating a collective security mechanism. The absence of a coordinated international legal response to the NotPetya attack reflects the ambiguity surrounding the legal characterization of such incidents, rather than constituting explicit legal acquiescence. However, this inaction arguably contributes to a normative vacuum that reinforces cyclical instability. This case underscores how asymmetries in cyber capabilities may incentivize more technologically advanced states to adopt preemptive measures, while less capable actors may respond defensively or asymmetrically, potentially contributing to escalation.

From both cases, it is obvious that the framework of international law established in the past is no longer applicable to today's international community. This is primarily because international law was designed for a global society where rights and obligations must be extended to all social entities. However, existing regulations concerning cyberattacks are limited in their practical applicability. The Tallinn Manual, while attempting to extend the armed character to cyberspace, has limited enforcement due to its non-binding nature. Therefore, cybersecurity governance must move beyond a zero-sum mentality to counteract the growing risk of anarchic behavior in cyberspace.

5. Breaking the Zero-Sum Dilemma: Exploring the Path from Confrontation to Cooperation

5.1. Differences in Cyber Governance within the Context of International Law

There is no doubt that the governance of cyberspace under the framework of international law has fallen into a structural zero-sum game. In this context, Western countries, led by the United States, advocate for the "Supremacy of Internet Freedom" and utilize the Tallinn Manual 2.0 to equate cyber attacks with traditional military actions,and are more inclined to invoke the right of anticipatory self-defense through preemptive cyber operations. Conversely, countries such as China and Russia advocate a perspective that emphasizes "Cyber Sovereignty". In 2020, China introduced the Global Data Security Initiative to underscore sovereign boundaries. It is not difficult to see that these positions reflect a dichotomy between developed network nations and emerging network powers, highlighting a fundamental structural confrontation. Just as in game theory, the two sides regard the rule-making right as a "Zero-Sum Battlefield" for interest, and any party's rule advantage means that the enemy's strategic space may be plundered. As a result of this zero-sum logic model, the two sides have not prioritized exploring cooperative governance solutions, and the institutional confrontation model is bound to intensify [14].

5.2. Refining the Rules of International Law

Scholar Gray noted that in the Nicaragua case, the court affirmed the perspective that the provisions of the Charter evolve dynamically in response to changes in state practice. Currently, the refinement of international law rules faces significant legal challenges arising from digital armed conflicts.

5.2.1. The Refinement of the Quantitative Standard

Generally, the refinement of the standard needs to be treated in a specific way. Adhering to fundamental principles and integrating a reasonable application of the principle of proportionality is essential for assessing consequences and confirming the composition of force. The eight-element principle serves as a framework for measuring and evaluating specific circumstances surrounding cyber operations, encompassing seriousness, intrusion, immediacy, state involvement, directness, presumptive legality, military nature, and measurable impact. This framework constitutes the foundational principles for assessment. Particularly critical is the element of seriousness; cyber operations must attain a certain threshold before they can be classified as an exercise of force. This classification is intrinsically linked to the nature of their consequences. The evaluation should correspond to factors such as immediacy, directness, intrusiveness, and measurability. For instance, if a cyber action occurs without another country's consent and intrudes upon its network infrastructure — potentially considered part of its territorial integrity — it creates an immediate situation whose consequences rapidly unfold. The likelihood that such actions will be justified as uses of force increases proportionally with any established causal link to substantial and quantifiable harm they may inflict.

As a typical case of the Stuxnet virus attack, some scholars cite the "Impact Measurability" standard, suggesting that Stuxnet virus attacks may be regarded as equivalent to conventional armed attacks, and their level can be considered to rise to the use of force.

Furthermore, certain scholars have underscored the importance of applying the principle of proportionality flexibly in this context.

In particular, the ICJ has further elucidated that proportionality is central to assessing the legality of using force. This principle requires evaluating the expected direct and tangible benefits of military operations against the potential civilian casualties and physical damage they may cause. An assault constitutes an offense only if it results in excessive harm.

5.2.2. Attribution Mechanism

In 2018, the UN adopted a resolution to establish the Open-ended Working Group (OEWG), which focuses on the following topics: norms, rules and principles of responsible actions of nations; The UN General Assembly endorsed a multi-stakeholder and expert-led initiative to work on norms governing cyber behaviour and provided suggestions in a workshop focused on attribution. Experts have proposed that attribution responsibility in cybersecurity should be comprehensively analyzed from three levels, including technical, legal, and political. Notably, from a political perspective, there is an emphasis on the intersection between state actors' behaviors and private actors' identities as tools and services utilized by states in cyberspace, particularly in cases involving commercial spyware, which raises critical questions about national accountability. Simultaneously, it explores how the International Criminal Court can hold individuals accountable at the international level for engaging private hacking groups. These matters significantly impact attribution processes and present promising avenues for further exploration.

5.3. Explore Ways for the Establishment of a Security Cooperation Mechanism in Cyberspace

5.3.1. Strengthen the Critical Infrastructure Defense Layer

As far as game theory is concerned, cyberattacks, as emerging tools that can supplement traditional warfare, offer certain advantages to the offensive party while inflicting detrimental effects such as economic losses and social insecurity on the targeted side. This dynamic explains why contemporary networked powers are increasingly inclined to adopt a "Pre-emptive" strategy. However, this approach has led to intense competition among various actors in cyberspace. Broadly speaking, both parties are so entrenched in competition for strategic advantages that no clear winner emerges once cyber conflict escalates. Consequently, an entirely open and secure cyberspace remains elusive.

From another perspective, if defenders can gain an advantage through effective defensive measures, actors may be more inclined toward cooperation. Thus, enhancing defense capabilities holds extraordinary significance. The case of the Stuxnet virus illustrates that attackers need only circumvent firewalls to inflict systemic damage. Some Chinese scholars have suggested that by strengthening defensive barriers, it is possible to effectively thwart viruses from causing further harm; this could be achieved by establishing early security warning mechanisms that act as alarms for identifying attacks. Such a defense-first strategy can effectively disrupt zero-sum thinking and — more importantly — better equip stakeholders to respond to viral threats.

5.3.2. Establishing a Community for Data Security and Implementing Confidence-Building Measures

At the United Nations Conference on Confidence-Building Measures (CBM) in 2024, A Chinese technology company proposed three initiatives to enhance the protection of global supply chains and critical information infrastructure (CII). The first proposal advocates for the promotion of objective security through the development of clear standards for supply chains, identification of common guidelines, and alignment with existing regional standards. Secondly, it emphasizes the creation of safe havens for CII and seeks to improve resource allocation by establishing designated protected areas. Finally, Huawei

suggests improving the global protocol for reporting and disclosing information and communication technology vulnerabilities. These initiatives aim to establish a three-tier linkage mechanism designed to enhance the overall security of cyberspace.

At the same time, A key international stakeholder's Global Data Security Initiative proposed a "Disable Backdoor" clause, which strictly suppressed the unequal mode of data sovereignty. This mechanism breaks away from the traditional logic of unilateral data control and shifts towards the co-creation of value within the network environment. This data community model belongs to the innovation of the governance model, This data community model represents an innovation in governance that, on one hand, ensures the integrity of national digital sovereignty and, on the other, maximizes the value of data. The above models are conducive to increasing mutual trust, conducive to carrying out effective cooperation, and achieve the purpose of mutual benefit and win-win.

The current cyberspace governance is gradually transforming to "System Co-construction", adopting a defense-first strategy to guide the reshaping of security concepts, using the data community model to restructure the pattern of interests. Additionally, countries are establishing a foundation of trust through technical cooperation. By integrating these two pathways, we can provide a viable framework for constructing a sustainable cyberspace community.

5.4. Practical Reflection on Non-Zero-Sum Logic

It is evident that in the contemporary era, network attacks frequently serve as an effective instrument for zero-sum games due to their characteristic of "low cost with high returns". and such asymmetry also significantly strengthens the tendency of powerful countries to maintain zero-sum thinking. A pertinent example is the exclusion of Huawei's 5G technology by the United States due to concerns over potential security risks in telecommunications infrastructure, which underscores broader competition over digital sovereignty.

The realization of the non-zero-sum logic inevitably means accepting the inevitability of some zero-sum conflicts, especially from NATO's classification of cyberspace as the "Fifth Operational Domain",This perspective underscores that technological superiority continues to be perceived as a fundamental element within the framework of zero-sum competition, thereby reflecting the growing militarization of cyberspace.

The question of whether a cyber attack constitutes the use of force is fundamentally a qualitative debate regarding "Digital Violence" within the framework of international law, Furthermore, the governance of security in cyberspace hinges on whether institutional innovation can outpace technological advantages. The application of a non-zero-sum model in this domain is not a panacea, but it is also far from theoretical rhetoric; rather, it represents a pragmatic middle path of compromise. This implies that the international community must accept limited conflict while prioritizing institutionalized cooperation to optimize shared interests, such as data sharing within the digital economy.Simultaneously, Since non-zero-sum logic is essentially dependent on the accumulation of mutual trust generated in repeated games, establishing a sustainable mechanism for trust-building becomes critically important.

6. Conclusion

Whether cyber attacks constitute the use of force in international law is challenged by both law and practice, and its ambiguity is amplified by the lag of international law, which encourages the spread of "Gray Zones" between countries. The zero-sum dilemma reflected in the current confrontation in cyberspace stems from the governance differences between the two mainstream camps, with one side more advocating "Internet Freedom" and the other more inclined to protect "Internet Sovereignty". To crack the differences, we need to break through the zero-sum logic, recognize the difference between the traditional identification of force and the characteristics of cyber attacks, combine the core principles

and refine the criteria for determining cyber force to make a comprehensive judgment, so as to restrain the abuse of unilateralism and "Preemptive", simultaneously build a governance model that integrates a strengthened defense system and an inclusive information community, and promote the network security governance from zero-sum confrontation to dynamic equilibrium. Transform the mentality based on absolute zero-sum competition into one of risk-sharing and information-sharing, so as to explore a sustainable double-win mechanism for both parties.

References

1. H. Eslam and G. Tiwari, "Cyberspace: Reimagining Cybersecurity and Its Impact on State Sovereignty," in *Cybercrime Unveiled: Technologies for Analysing Legal Complexity*, Cham, Switzerland: Springer Nature, 2025, pp. 93–112, doi: 10.1007/978-3-031-80557-8_4.
2. A. Chander and H. Sun, "Sovereignty 2.0," *Vand. J. Transnat'l L.*, vol. 55, pp. 283, 2022, doi: 10.2139/ssrn.3904949.
3. M. Saaida, "Digital Sovereignty," *Sci. For All Publ.*, vol. 6, no. 1, pp. 1–12, 2023, doi: 10.14763/2020.4.1532.
4. A. Bogdanchikova, "The Prisoners' Dilemma of the Cyber Relations between the European Union and Russia," 2022.
5. M. Murniasari, "China's Cybersecurity Governance as Part of Foreign and Security Policy," *Security Intell. Terrorism J.*, vol. 1, no. 2, pp. 94–107, 2024, doi: 10.70710/sitj.v1i2.23.
6. M. Jiang, "Chinese Cybersecurity Policies in the Age of Cyber Sovereignty," in *Quo Vadis, Sovereignty? New Conceptual and Regulatory Boundaries in the Age of Digital China*, Cham, Switzerland: Springer Nature, 2023, pp. 77–90, doi: 10.1007/978-3-031-41566-1_5.
7. Z. F. Rao, "Human-Centric Cybersecurity: Safeguarding Individuals in the Digital Age," 2024.
8. D. Broeders, F. Cristiano, M. Kaminska *et al.*, "In search of digital sovereignty and strategic autonomy: Normative power Europe to the test of its geopolitical ambitions," *J. Common Mark. Stud.*, vol. 61, no. 5, pp. 1261–1280, 2023, doi: 10.1111/jcms.13462.
9. H. Huang, "Digital Diplomacy in Cyberspace Governance," in *China's Diplomacy and Int. Law*, Singapore: Springer Nature, 2024, pp. 269–310, doi: 10.1007/978-981-97-1968-6_8.
10. C. Chen and B. Dong, "Digital forensics analysis based on cybercrime and the study of the rule of law in space governance," *Open Comput. Sci.*, vol. 13, no. 1, p. 20220266, 2023, doi: 10.1515/comp-2022-0266.
11. D. Huang, "40 Years of China's International Governance in Cyberspace," in *Research on the Rule of Law of China's Cybersecurity: China's Rule of Law in Cybersecurity Over the Past 40 Years*, Singapore: Springer Nature, 2022, pp. 139–171, doi: 10.1007/978-981-16-8356-5_4.
12. J. Burton and G. Christou, "Bridging the gap between cyberwar and cyberpeace," *Int. Aff.*, vol. 97, no. 6, pp. 1727–1747, 2021, doi: 10.1093/ia/iiab172.
13. S. Kim, "The Inter-network Politics of Cyber Security and Middle Power Diplomacy: A Korean Perspective," in *Korea's Middle Power Diplomacy: Between Power and Network*, Cham, Switzerland: Springer Int. Publ., 2022, pp. 97–123, doi: 10.1007/978-3-030-76012-0_6.
14. T. Manuwa, "Analysis of the Impact of Cyber-Diplomacy on International Relations," *J. Public Admin. Manag.*, vol. 2, no. 4, pp. 1–9, 2023.