`Cadernos de Pós-Graduação em Direito Político e Econômico
ISSN 1678-2127 (Print)
ceapress.org/index.php/cpgdpe
Volume 26 · Issue 3 · 2026
Pages 1–8

The Problematics of Applying the Principle of Non-Intervention in International Law to Cyberspace: An Analytical Study in Light of Contemporary State Practice

Dr. Mellah Nassira*[1], Dr. Saou Houria[2]

[1] M'Hamed Bougara University of Boumerdes, Algeria. Email: na.mellah@univ-boumerdes.dz

[2] University of Chlef, Algeria. Email: h.saou@univ-chlef.dz

Received: 28/07/2026 | **Accepted:** 03/10/2026 | **Published:** 12/11/2026

***Abstract*—**This study aims to analyze the legal and practical challenges associated with applying the traditional principle of non-intervention in international law to cyberspace, in light of the growing number of state-conducted cyber operations that threaten the sovereignty and stability of other states. The paper examines the gap between the relative stability of international legal norms and the dynamic, rapidly evolving nature of cyber threats, through an analysis of recent state practice, most notably alleged electoral interference and attacks on critical infrastructure. It argues that the current legal framework requires the development of clearer and more operationalizable standards to adapt the principle of non-intervention to the realities of the digital domain, and proposes a framework to strengthen mechanisms of accountability and deterrence.

***Keywords*—**Principle of Non-Intervention; Cyberattacks; State Sovereignty; International Responsibility.

Résumé :

Cette étude vise à analyser les défis juridiques et pratiques associés à l'application du principe traditionnel de non-intervention en droit international au cyberespace, à la lumière du nombre croissant d'opérations cybernétiques menées par des États qui menacent la souveraineté et la stabilité d'autres États. L'article examine l'écart entre la stabilité relative des normes juridiques internationales et la nature dynamique et en évolution rapide des cybermenaces, à travers une analyse de la pratique étatique récente, notamment les interférences électorales alléguées et les attaques contre les infrastructures critiques. Il soutient que le cadre juridique actuel nécessite le développement de normes plus claires et opérationnalisables afin d'adapter le principe de non-intervention aux réalités du domaine numérique, et propose un cadre pour renforcer les mécanismes de responsabilisation et de dissuasion.

Mots-clés : Principe de non-intervention ; Cyberattaques ; Souveraineté de l'État ; Responsabilité internationale.

INTRODUCTION:

The international system has undergone profound transformations over recent decades as a result of the digital revolution, which has reshaped patterns of interaction among states and shifted a significant part of the exercise of power and influence into cyberspace. Threats are no longer confined to traditional forms associated with the use of military force. New forms of international conduct have emerged, characterized by their intangible nature, speed, and complexity, creating unprecedented challenges for international law, foremost among them the principle of non-intervention, one of the fundamental pillars governing relations among states.

The United Nations enshrined this principle in its Charter as part of its effort to ensure respect for state sovereignty and prevent any infringement of political independence. However, the digital environment has generated practices that are difficult to classify within traditional legal categories because of attribution

How to cite: Nassira & Houria (2026). The Problematics of Applying the Principle of Non-Intervention in International Law to Cyberspace: An Analytical Study in Light of Contemporary State Practice. `Cadernos de Pós-Graduação em Direito Político e Econômico, 26(3), 1–8.
© 2026 The Author(s). Published by Centro de Estudos Acadêmicos Press [ceapress.org].

uncertainty, the involvement of multiple actors, and different levels of impact. This raises genuine questions about the scope of protection afforded by the principle when confronted with cyber activities that may have profound effects without amounting to the use of force in the traditional sense.

The divergence between the relative stability of international legal texts and the rapid development of technological tools has deepened the difficulties involved in legally characterizing such acts, particularly in the absence of clear international consensus on the standards governing conduct in cyberspace. These difficulties have been intensified by practices targeting democratic processes and critical infrastructure, reflecting a qualitative shift in the tools used to exert political influence across borders.

Against this background, there is a need to reread the principle of non-intervention in a changing digital environment through an analytical approach, in order to assess the adequacy of the existing legal framework and identify ways of developing it to achieve greater clarity and effectiveness in addressing contemporary cyber challenges.

I. RESEARCH PROBLEM

The central problem lies in the contradiction between an abstract legal principle and a complex practical reality. Although the principle of non-intervention, as a rule of customary international law, prohibits states from intervening in the internal affairs of other states, its application to cyberspace faces several fundamental challenges:

1. Difficulty of attribution: It is difficult to prove that a particular cyber operation originates from a specific state in an official capacity, in a manner that would permit that state to be held legally accountable.

2. Unclear threshold: There is no clear and internationally agreed legal standard for distinguishing acceptable cyber activity, such as traditional espionage, from prohibited intervention, such as attempts to influence electoral outcomes.

3. The nature of cyberspace: Cyberspace is transnational and crosses borders, making the identification of "cross-border intervention" more ambiguous than intervention in the physical world.

4. Regulatory gap: There is no comprehensive, binding international treaty governing state conduct in cyberspace, leaving interpretation largely to unilateral state practice.

II. RESEARCH QUESTION

How can the principle of non-intervention in international law be adapted to address the challenges posed by contemporary state cyber practices, and what means can be employed to achieve effective accountability in this field?

III. RESEARCH METHODOLOGY

This study adopts an integrated methodological approach combining descriptive and comparative methods. The descriptive method identifies and analyzes the characteristics of cyberspace as a contemporary arena of international interaction by examining the nature and development of cyber operations and related threats, particularly those affecting state sovereignty and stability, such as attacks on critical infrastructure and interference in electoral processes. The comparative method compares the traditional application of the principle of non-intervention in international law with attempts to apply it to the cyber domain.

IV. OBJECTIVES OF THE STUDY

This paper seeks to analyze the legal and practical challenges facing the principle of non-intervention in cyberspace by examining prominent digital conflicts, with particular emphasis on the interaction among the state, non-state actors, and global digital infrastructure. It also aims to propose practical solutions to strengthen state sovereignty and protect digital neutrality, taking into account recent developments in cyberwarfare and cross-border cyberattacks.

V. SIGNIFICANCE OF THE STUDY

The significance of this study derives from the novelty of its subject and its considerable complexity. Cyberattacks, in particular, pose a formidable challenge to the established rules of customary international law concerning state sovereignty, the principle of non-intervention, and international responsibility. This, in turn, drives the emergence of new and evolving state practices aimed at addressing cyberattacks.

VI. STRUCTURE OF THE STUDY

Chapter One: The Conceptual Framework of the Study

The principle of non-intervention is one of the fundamental principles of international law, serving as an essential guarantee of respect for the sovereignty and independence of states in managing their internal and external affairs free from external pressure or influence. It was enshrined in the Charter of the United Nations, reflecting the international community's commitment to maintaining stability and preventing conflicts among states.

Rapid technological development, particularly in the digital domain, has generated new threats, most notably cyberattacks, which increasingly affect states' critical infrastructure and undermine their security and stability without recourse to conventional military force. This shift raises profound questions about whether the principle of non-intervention applies to such intangible acts and whether it constitutes a sufficiently robust legal framework for regulating them.

Section One: The Principle of Non-Intervention in International Law

The principle of non-intervention may be defined as the obligation to refrain from interfering in the internal or external affairs of any state, including through military, political, or economic intervention. Non-intervention in the domestic affairs of states is a fundamental principle of public international law. It is reflected in the Charter of the United Nations, particularly Articles 2(4) and 2(7), with the aim of protecting state sovereignty and political independence. Article 2(4) provides that "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state" (Charter of the United Nations, 1945, Article 2(4), p. 11). According to Brooks, the principle protects the political will of states and is not limited to geographical territory (Brooks, 2018, p. 34).

Despite its legal stability, this principle was not originally designed to address modern digital threats that transcend geographical borders, such as cyberattacks targeting critical infrastructure, electoral systems, and government communications. With the emergence of cyberspace as a strategic instrument for states, a new challenge has arisen, requiring reconsideration of national sovereignty and the means by which states can be protected against cyber intervention. Digital attacks are not merely technological crimes; they may also serve as instruments of political and economic pressure that affect the will of the targeted state (Brooks, 2018, p. 36).

Section Two: Cyberattacks

Cyberattacks are unauthorized operations targeting a state's information systems or critical facilities. They may range from data theft to the disruption of essential services. Their principal characteristics include the following (Schneider, 2019, pp. 52–53):

- **Geographical boundarylessness:** They can be carried out from anywhere in the world without physical entry into the targeted state.
- **Concealment and complexity:** Their source is often unknown or disguised through intermediary networks.
- **Multiplicity of actors:** The actors may include states, non-governmental groups, or private companies.

These characteristics make it difficult to apply traditional legal texts literally, since those texts were not designed to address cross-border digital attacks. According to McTaggart, international law has not developed sufficiently to accommodate cyber intervention that does not involve the traditional use of force, although it may be applicable through a broad interpretation of concepts such as coercive conduct (McTaggart, 2020, p. 78).

Recent studies suggest that traditional international law is no longer sufficient to confront modern digital threats. The classical principle of non-intervention focused on direct military and political interference within another state, but did not account for cross-border cyberattacks capable of disrupting critical infrastructure, influencing elections, or compromising sensitive government data (Moulin, 2020, pp. 215–220). Some scholars argue that the principle should be revitalized to incorporate cyberspace as part of national sovereignty, so that any digital act threatening a state's will or essential functions is regarded as prohibited intervention. This requires a clear legal framework for identifying cyber intervention. Digitalization also reshapes sovereignty itself: modern societies rely on digital infrastructure to manage their affairs, making intervention in cyberspace directly consequential for a state's political and economic functions.

Chapter Two: The Problem of Applying the Principle of Non-Intervention to Cyberspace

Section One: The Emergence of Cyberwarfare and the Transformation of International Conflict

Since the mid-2000s, the international system has undergone a structural transformation in the nature of conflict, as cyberspace has emerged as a new strategic domain in which power is exercised and conflicts are conducted. Power is no longer confined to traditional military instruments; it also includes “cyber power”, the use of digital technology to achieve political and security objectives through disruption, influence, or coercion (Nye, 2017, pp. 42–45). This transformation reflects the distinctive characteristics of cyberspace, particularly intangibility, exceptional speed, and the ability to transcend geographical borders. These features have produced a new form of conflict marked by ambiguity and complexity, often situated in the “grey zone” between peace and war (Kello, 2017, pp. 14–18).

The cyberattacks targeting Estonia in 2007 and Georgia in 2008 are prominent examples. In Estonia, distributed denial-of-service (DDoS) attacks caused widespread disruption to digital infrastructure, including government websites, financial institutions, and media outlets, directly affecting the state’s ability to perform essential functions. This was not merely a temporary technical malfunction; it amounted to a form of “functional paralysis of the state”, as institutions became unable to manage economic and security affairs normally, producing effects comparable in some respects to conventional attacks (Schmitt, ed., 2017, Rule 15, p. 213).

The Georgian case involved more complex cyber operations, as they coincided with Russian military operations in South Ossetia. This demonstrated the integration of cyber and military dimensions within “hybrid warfare”, whereby digital means are used to disrupt communications and control the information environment before and during operations on the ground (Rid, 2013, pp. 13–20).

The significance of these cases lies not only in their material or functional effects, but also in the profound legal questions they raise, foremost among them legal attribution, an essential condition for activating the rules of international responsibility. Unlike traditional attacks, cyber operations are difficult to trace to a precise source because they rely on globally distributed infrastructure and identity-concealment technologies such as virtual private networks (VPNs) and botnets. Attacks may also be routed through servers in several states without those states’ knowledge. This complicates the distinction between the actual perpetrator and the entity to which responsibility may legally be attributed, particularly when states use non-state actors as proxies, preserving a margin of “plausible deniability” (Kastenberg, 2009, pp. 47–50).

A further attribution challenge arises from the multiplicity of actors. Attacks may originate from non-governmental groups or actors informally supported by a state, creating a legal gap in determining responsibility. Contemporary state practice therefore points to the need for independent international investigative mechanisms capable of documenting technical evidence and linking it to the principle of non-intervention in order to ensure effective accountability (Dolan, 2022, pp. 119–120).

The problem becomes more complex when distinguishing technical attribution, which identifies the physical source of an attack, from legal attribution, which requires proof of an actual relationship between the actor and the state under internationally recognized standards, such as the “effective control” test adopted by the International Court of Justice. It may be possible to identify the technical route of an attack without conclusively proving the involvement of a particular state, weakening the application of international responsibility or the invocation of self-defence (Tallinn Manual 2.0, p. 120).

Cyberspace also raises questions about the legal characterization of attacks. International legal scholarship remains divided over whether certain cyber operations, such as DDoS attacks, constitute cybercrimes or may rise to the level of a “use of force” or even an “armed attack” under the UN Charter. This characterization often depends on an effects-based test, measuring the seriousness of an attack by its impact on a state’s critical infrastructure rather than solely by its technical nature (Schmitt, 2017, pp. 12–15). The absence of a uniform international standard makes such assessments susceptible to divergent state interpretations and undermines the possibility of a stable legal regime.

The emergence of cyberwarfare has therefore not merely introduced a new instrument into international conflict; it has profoundly reshaped the concepts of power, sovereignty, and responsibility, imposing unprecedented challenges on traditional international law. This calls for a legal approach capable of accommodating the dynamic nature of cyberspace while balancing international security and respect for state sovereignty in the digital age.

Section Two: Cyber Neutrality and the Problem of Its Application in International Law

Neutrality is an established principle of traditional international law. It requires states that do not participate in an armed conflict to refrain from supporting any party, in return for protection against hostile acts. The rules of neutrality were developed in the 1907 Hague Conventions, which defined the obligations of neutral states, particularly refraining from military assistance or allowing their territories to be used as a base for hostile operations. The transfer of conflicts into cyberspace has, however, raised new challenges.

Unlike the traditional environment, cyberspace has no clearly defined geographical borders within which a state can exercise exclusive sovereignty. It relies on distributed digital infrastructure, much of which is managed by transnational private companies. A state may consequently become an indirect party to a cyber conflict unintentionally, simply because its digital infrastructure is used to conduct attacks or defend against them. The central issue is whether traditional neutrality can be reconciled with a domain in which complete abstention from involvement is difficult to achieve.

The 2008 Georgian case illustrates this complexity. While facing intensive cyberattacks, the Georgian government moved its official websites to servers in the United States and relied on American technology companies to secure its digital infrastructure. Although the US government did not officially intervene, technical support provided by private companies raised questions about state neutrality, particularly in the absence of a clear legal framework governing state responsibility for the acts of non-state actors within its territory (Shackelford, 2009, p. 193).

Another legal challenge is whether the use of a neutral state's digital infrastructure to conduct cyber operations violates neutrality obligations. Traditional international law requires a neutral state to prevent its territory from being used for military purposes by parties to a conflict. Applying this obligation in cyberspace is difficult because digital networks are decentralized and all activities passing through them are hard to monitor. Measures to prevent such activities may require complex technical interventions and raise issues concerning freedom of Internet use and the rights of private actors (Kastenberg, 2009, pp. 47–50).

The relationship between the state and the private sector also raises questions, since technology companies play a central role in managing and operating global digital infrastructure. This prompts inquiry into whether such companies are bound by neutrality rules and whether their conduct may be attributed to their home state. Under international responsibility rules, the conduct of non-state actors is attributable to a state only where a certain degree of control or direction exists. This condition is difficult to prove in most cyber cases, creating a legal grey area that weakens neutrality (Tallinn Manual 2.0, p. 124).

The concept of "cyber neutrality" raises deeper questions about whether traditional rules can adapt to a digital environment characterized by interconnectedness. Traditional neutrality assumes a clear distinction between belligerent and non-participating states, whereas cyberspace blurs this distinction as interests and infrastructure intersect, making neutrality relative rather than absolute. Some scholars consequently argue that neutrality in cyberspace is no longer merely a negative obligation to abstain, but also entails positive obligations, such as measures to prevent national infrastructure from being used for hostile acts (Moulin, 2020, pp. 423–447).

Adopting this approach raises concerns about the ability of states, particularly developing countries, to meet technical obligations and about the risks of expanding their international responsibility. It may also lead to "cyber surveillance" that conflicts with the free flow of information, leaving states to balance cybersecurity requirements against respect for digital rights.

Cyber neutrality is therefore one of the most problematic concepts in contemporary international law, exposing a gap between traditional legal rules and the practical realities of the digital environment. A new legal approach is needed that takes account of cyberspace, redefines state obligations, determines the responsibilities of non-state actors, and strengthens international cooperation to ensure respect for neutrality in a complex digital environment.

Chapter Three: International Responsibility in Cyber Conflicts

International responsibility is one of the most complex issues in cyber conflicts, given the challenges relating to the nature of the wrongful act, the identity of the actor, and the limits of legal attribution. Under traditional international law, state responsibility arises where an act attributable to a state constitutes a breach of an international obligation, as set out in the International Law Commission's 2001 Articles on Responsibility of States for Internationally Wrongful Acts. Applying this framework to cyberspace presents structural difficulties arising from the ambiguity and technical complexity of this domain.

The first difficulty concerns attribution. Establishing a link between a cyber act and a state is essential to determining responsibility. Yet cyberattacks rely on identity-concealment technologies and globally distributed intermediary networks, making it difficult to identify the perpetrator accurately. This creates what may be called an "evidentiary crisis" in international cyber law and weakens accountability through diplomatic or judicial channels (Kastenberg, 2009, pp. 50–52).

The problem also extends to the legal characterization of a cyber act, namely, determining whether it constitutes a breach of an international obligation. Cyberattacks may range from digital espionage and information sabotage to interference in political processes. This raises questions about the criteria for distinguishing lawful from unlawful conduct. The absence of international consensus on clear definitions of "cyberattack" or "unlawful intervention" further complicates responsibility (Schmitt, 2017, pp. 20–22).

State responsibility for the acts of non-state actors presents an additional challenge, given their growing role in cyber operations. Under traditional rules, the conduct of individuals or groups is attributable to a state only where a certain degree of control or direction exists, a condition difficult to establish in the cyber context. This has created "legal grey areas" in which attacks with serious consequences are carried out without a clear possibility of holding a particular entity accountable, threatening the effectiveness of the international legal system.

Another issue concerns the possibility of invoking the right of self-defence in response to cyberattacks. The UN Charter requires an "armed attack" for this right to be invoked. Whether cyberattacks can reach this threshold remains debated, particularly where they cause no direct physical damage despite significantly affecting critical infrastructure or national security.

These challenges demonstrate the need for a clearer and more flexible international legal framework that takes account of cyberspace, strengthens international cooperation in investigation and tracing, and establishes common standards for determining responsibility, while balancing international security and respect for state sovereignty.

Section One: Cyber Intervention in Electoral Processes and the Reshaping of Sovereignty

The development of cyberspace has generated new forms of intervention in the internal affairs of states, particularly through attempts to influence electoral processes and political debate. This phenomenon has generated extensive debate in international legal scholarship because of the challenges it poses in determining the scope of non-intervention and the limits of sovereignty in the digital age.

One scholarly approach calls for reinterpretation of non-intervention in light of self-determination, so that protection extends beyond state institutions to include the people as the source of political legitimacy. Under this view, interventions targeting elections or influencing voters' will constitute a direct violation of sovereignty, even where they do not target official state infrastructure. This shifts the focus from the state as an institution to the people as a fundamental actor in forming political authority (Willmer, 2023, pp. 112–114).

Another approach calls for strengthening digital sovereignty by imposing restrictions on foreign intervention in the information environment, whether by regulating digital content or requiring transparency about its sources. This approach seeks to protect domestic debate from external influence, particularly amid growing media disinformation and information manipulation. However, it raises concerns about restrictions on freedom of expression and the possibility of using it as a pretext for controlling the digital sphere (Pijpers, 2025, pp. 32–36).

The divergence between these approaches reveals a deeper problem concerning the balance between protecting sovereignty and ensuring digital openness. Given the transnational nature of the Internet, the domestic and external spheres can no longer be clearly separated. International law must therefore reconsider its traditional concepts and theoretical foundations in light of digital transformations.

Section Two: Towards Developing the Principle of Non-Intervention in Cyberspace

In light of the growing challenges posed by cyberspace, it is necessary to reconsider the principle of non-intervention, not by abandoning it, but by developing and adapting it to the new digital reality. This requires a comprehensive approach combining legal, technical, and political dimensions to build an international framework capable of effectively regulating conduct in cyberspace.

First, basic legal concepts must be clarified by developing precise definitions of "cyberattack", "unlawful intervention", and "use of force in the digital domain". Such clarification is essential to reducing legal ambiguity and enhancing the applicability of international rules.

Second, international cooperation must be strengthened through the exchange of information on cyber threats, the development of joint investigative and tracing mechanisms, and the establishment of multilateral platforms for coordinating responses. Practical experience demonstrates that individual state efforts are insufficient to confront inherently transnational cyber threats (Moulin, 2020, pp. 221–223).

Third, the rules governing the use of force should be reconsidered to allow cyber acts with significant effects to fall within their scope, while taking the specific characteristics of cyberspace into account. This requires objective criteria for determining the "threshold of force", balancing the prevention of escalation with states' right to defend themselves.

Finally, non-state actors should be integrated into the international legal framework by defining their responsibilities and establishing rules governing their role in cyberspace, particularly in view of their growing influence.

CONCLUSION:

The foregoing analysis demonstrates that cyberspace has not merely brought about a technological change in international conflicts; it has profoundly reshaped the fundamental concepts underlying international law, foremost among them sovereignty, non-intervention, and international responsibility. Cyber conflicts have exposed the limits of traditional rules and their inability to accommodate the complexities of this new domain.

This reality does not mean the collapse of the international legal system. Rather, it creates an opportunity to develop and modernize that system in a manner consistent with contemporary transformations. The principal challenge remains achieving a balance between cybersecurity requirements, respect for state sovereignty, and preservation of an open digital environment within an international system based on cooperation and coordination.

Accordingly, the future of international law in the digital age depends on the international community's ability to establish common rules based on a profound understanding of cyberspace and responsive to the requirements of stability and justice in the international system.

First: Findings

1. Cross-border cyberattacks affect not only traditional infrastructure but also a state's political will and essential functions, calling for a redefinition of non-intervention in international law.
2. The difficulty of accurately identifying the source of cyberattacks, together with the use of non-state actors, creates a legal gap in attributing responsibility to states and complicates the application of the right of self-defence.
3. The distributed nature of digital networks makes traditional neutrality incapable of absolute application and requires positive measures to prevent national infrastructure from being used in cyber conflicts.
4. Ensuring the effectiveness of non-intervention requires precise definitions of cyberattacks and unlawful intervention, stronger international cooperation, reconsideration of the rules on the use of force, and the integration of non-state actors into the framework of legal responsibility.

Second: Recommendations

5. Develop joint international mechanisms for monitoring and verifying cyberattacks, including information exchange among states and international organizations.
6. Strengthen national and international laws defining state responsibility in relation to non-state actors, while ensuring the protection of cyber neutrality.
7. Reformulate the rules governing the use of force to encompass impactful digital operations, while ensuring compliance with international law and the protection of human rights.

Prospects of the Study:

This study opens promising horizons for legal scholarship and international policy by establishing a critical foundation to bridge the normative gap between traditional public international law and the fluid reality of cyberspace. Beyond diagnosing the inadequacies of the classical non-intervention principle, it paves the way for drafting binding multilateral instruments or UN-backed interpretive guidelines that clearly delineate the legal thresholds of digital coercion and operationalize standards for the use of force. Furthermore, it stimulates prospective research into reconciling digital forensics with legal standards of evidence, establishing joint international attribution mechanisms, and integrating the accountability of non-state proxies. Ultimately, these

prospects provide a vital roadmap for future inquiries aimed at recalibrating state sovereignty and the law of neutrality to safeguard critical digital infrastructure without undermining human rights, internet freedom, and the open flow of information.

REFERENCES:

1. Charter of the United Nations (1945). United Nations, Articles 2(4) and 2(7).
2. Brooks. (2018). International Law and Non-Intervention. Cambridge University Press.
3. Schneider, T. (2019). Cyber Threats and Sovereignty. Routledge.
4. McTaggart, A. (2020). “Cyber Operations and International Law.” Global Security Review.
5. Moulin, T. (2020). “Reviving the Principle of Non-Intervention in Cyberspace.” Journal of Conflict and Security Law, 25(3).
6. Nye, J. (2017). The Future of Power. New York: Public Affairs.
7. Kello. (2017). The Virtual Weapon and International Order. New Haven: Yale University Press.
8. Schmitt, M. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press.
9. Rid, T. (2013). Cyber War Will Not Take Place. Oxford: Oxford University Press.
10. Dolan, M. (2022). “State Responsibility in Cyberspace.” Journal of International Law.
11. Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press.
12. Shackelford, S. J. (2009). “From Nuclear War to Net War: Analogizing Cyber Attacks in International Law.” Berkeley Journal of International Law, 27(1).
13. Moulin, T. (2020). “Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward.” Journal of Conflict and Security Law, 25(3).
14. Ziolkowski, K. (2013). “General Principles of International Law as Applicable in Cyberspace.” In Peacetime Regime for State Activities in Cyberspace. Tallinn: NATO CCD COE Publications.
15. Safi, S. (2020). Sovereignty in Cyberspace: A Study on Customary International Law on the Principle of Sovereignty.
16. Kastenberg, J. E. (2009). “Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law.” Air Force Law Review.
17. Willmer, L. (2023). “Does Digitalization Reshape the Principle of Non-Intervention?” German Law Journal, 24(3).
18. Pijpers, P. B. (2025). “Disinformation in Cyberspace: Principles of Sovereignty and Non-Intervention under International Law.” The Military Law and the Law of War Review, 63(1).