International Responsibility of States for Cyberattacks against Countries' Critical Infrastructure

1. Kiana Abdi*: Master of International Law, Department of Law, University of Tehran, Tehran, Iran

*Correspondence: Abdikiyana021@gmail.com

Abstract

Cyberattacks against countries' critical infrastructure have become one of the most significant challenges of international law over the past two decades. Using a descriptive-analytical method, this article examines the international responsibility of states for such attacks. The research findings indicate that, despite the consolidation of the general principles of responsibility in classical law, establishing responsibility in cyberspace faces two fundamental obstacles: first, the difficulty of proving the attribution of attacks to states due to the intangible and transboundary nature of cyberspace, the possibility of identity falsification, and the use of non-state actors by states; and second, the absence of clear and uniform standards regarding the level of evidence required to prove cyberattacks. State practice in the cases of Stuxnet and attacks on Ukraine's infrastructure shows that states often refrain from accepting responsibility and resort to a strategy of denial. If responsibility is established, its legal consequences include cessation of the wrongful act, reparation for damage, and countermeasures, each of which faces practical implementation challenges. Finally, the article presents proposals for drafting a comprehensive international treaty, establishing an independent body for investigating cyberattacks, and developing evidentiary standards.

Keywords: international responsibility of states, cyberattacks, critical infrastructure, attribution, evidentiary standards

Received: 24 March 2026
Revised: 14 June 2026
Accepted: 25 June 2026
Initial Publication 26 June 2026
Final Publication 01 May 2027

Citation: Abdi, K. (2027). International Responsibility of States for Cyberattacks against Countries' Critical Infrastructure. *Legal Studies in Digital Age*, 6(3), 1-10.

1. Introduction

Cyberspace, as the fifth strategic domain after land, sea, air, and outer space, has, over the past two decades, become an arena for geopolitical competition and even covert confrontations among states. Countries' critical infrastructure—including energy, water, transportation, communications, and nuclear facilities—which was once exposed only to physical threats, is now targeted by sophisticated cyberattacks. These attacks can not only cause widespread disruption to public order and national security, but in some cases may also lead to loss of life and physical destruction of facilities. Technical complexity, the relative anonymity of attackers, and the speed of data transmission have confronted international law with unprecedented challenges in determining the boundaries of responsibility. Accordingly, the issue of attributing a cyberattack to a specific state and

subsequently imposing international responsibility on that state has become one of the most sensitive and controversial questions in contemporary law (Schmitt, 2021).

Despite remarkable advances in information technology, public international law still faces serious gaps in regulating cyberattacks. The Budapest Convention, adopted in 2001, as the most important international instrument in the field of cybercrime, mainly focuses on police and judicial cooperation and remains unable to address state-sponsored attacks against the critical infrastructure of other countries. On the other hand, the United Nations Charter and the Draft Articles on Responsibility of States for Internationally Wrongful Acts, prepared by the International Law Commission in 2001, although outlining the general framework of responsibility, do not provide specific rules for cyberattacks that are intangible and transboundary in nature. This legal gap has led states in practice to resort to political mechanisms, cyber retaliatory measures, and even threats of the use of force instead of judicial remedies, which may itself endanger international stability (Crawford, 2013).

The fundamental challenge in establishing the international responsibility of states in this field is proving the causal relationship between the conduct of a state and the cyber incident that has occurred. Unlike classical military attacks, which can be traced through tangible evidence such as flight traces or firing traces, cyberattacks can be carried out through intermediary servers, computers controlled by third parties, or even by falsifying Internet Protocol addresses. This issue has made the application of traditional evidentiary standards, such as "effective control," which was crystallized in the judgment of the International Court of Justice in the Nicaragua case in 1986, extremely difficult. For this reason, leading jurists have emphasized the need to develop evidentiary standards appropriate to the nature of cyberspace, such as the "clear and convincing evidence" standard or the use of technical and expert evidence verified by neutral international bodies (Roscini, 2014).

In addition to the issue of attribution, another element of responsibility, namely the breach of an international obligation, has also become open to interpretation in cyberattacks against critical infrastructure. The International Court of Justice, in the Oil Platforms case in 2003 and the Armed Activities in the Congo case in 2005, introduced the criterion of "severity of effects" for determining the breach of an obligation and even the use of force. The question arises whether cyberattacks that lead to widespread power outages, disruption of the banking system, or paralysis of a country's air transport network can constitute "aggression" or "use of force" within the meaning of Article 2(4) of the United Nations Charter. Many states and jurists believe that if the physical consequences of a cyberattack are equivalent to those of a traditional armed attack, it may be regarded as a "use of force," and the victim state's right of self-defense may be recognized under Article 51 of the Charter (Dinstein, 2017). However, this interpretation has not yet developed into a uniform international practice and remains a matter of serious disagreement among states.

From the perspective of state practice, numerous incidents, such as the cyberattack on Iran's nuclear facilities in 2010, known as Stuxnet, the attacks on Ukraine's power grid in 2015 and 2016, and also the cyber assassination of political and nuclear figures, have shown that states often refrain from formally accepting responsibility or, after formally declaring attribution, respond outside the framework of legal institutions. The United Nations Groups of Governmental Experts on state behavior in cyberspace, as well as the Open-ended Working Group in the same field, despite years of effort, have been unable to develop a comprehensive and binding treaty in this area and have merely formulated a set of non-binding rules that do not possess the necessary effectiveness in deterrence and reparation (Ghorbani, 2022). This situation has placed states in a period of legal ambiguity and insecurity, revealing the urgent need to reconsider the foundations of responsibility and present operational solutions.

Accordingly, the present article, using a descriptive-analytical research method and relying on authoritative sources of international law, judicial practice, and reports of international institutions, seeks to answer the fundamental question of under what conditions, within the existing legal system, the international responsibility of states for cyberattacks against critical infrastructure is established, and what shortcomings and ambiguities exist in this process. The main hypothesis of the study is that, despite the consolidation of the general principles of responsibility in international law, the difficulty of proving attribution and the absence of transparent criteria for assessing the severity of effects constitute the major obstacles to establishing state responsibility in this field, and overcoming these obstacles requires the adoption of a cyber-specific international instrument and the enhancement of transnational technical-judicial cooperation. Finally, this article will offer solutions for the legal

policymaking of states, particularly the Islamic Republic of Iran, in confronting this challenge, in order to take at least a small step toward clarifying this complex legal field (Zemanek, 2018).

2. Research Method

The present study uses a descriptive-analytical research method with a legal approach to examine the international responsibility of states for cyberattacks against countries' critical infrastructure. The descriptive-analytical method, as one of the most common research methods in the humanities, particularly in law, makes it possible to examine existing concepts, rules, and practices systematically and in depth. In this method, the required data were first collected through library-based tools, authoritative international instruments, and written sources, and were then examined and interpreted through an analytical and critical approach. Among the most important sources used in this study are the Draft Articles on Responsibility of States for Internationally Wrongful Acts, Tallinn Manual 2.0, reports of United Nations working groups in the field of cyberspace, the judicial practice of the International Court of Justice, and authoritative books and articles on international law in both Persian and English. Moreover, in order to better understand the existing challenges, concrete examples of cyberattacks such as Stuxnet and attacks on Ukraine's infrastructure were analyzed as case studies. In terms of nature and objective, this research is applied, because its results may be used in the legal policymaking of states, especially the Islamic Republic of Iran, in confronting cyberattacks and drafting relevant domestic and international rules.

3. Concepts and Theoretical Foundations

To enter the discussion of the international responsibility of states for cyberattacks against critical infrastructure, it is first necessary to establish a clear conceptual framework for the fundamental concepts of this field. These concepts include the definition of cyberattack and critical infrastructure, the explanation of the legal nature of cyberspace, and the identification of the foundations of the international responsibility of states in classical law. Without an accurate understanding of these concepts, a coherent legal analysis of the elements of responsibility, attribution, and breach of obligation will not be possible. Therefore, in this section, each of these concepts is briefly examined (Ziaei Bigdeli, 2019).

The definition of cyberattack and critical infrastructure has long been one of the fundamental challenges of international law in the field of cyberspace. The absence of a single and binding definition at the global level has caused states to adopt different practices in identifying instances of cyberattacks and determining the scope of critical infrastructure. In European Union instruments, Directive 2016/1148 describes a "cyber incident" as any event that disrupts the security of network and information systems, and defines critical infrastructure as facilities and systems whose disruption or destruction would have a significant effect on national security, public health, the economy, or the social order of member states. Directive 2022/2555 also emphasizes that critical infrastructure includes the sectors of energy, transport, banking, health, drinking water, wastewater, digital infrastructure, public administration, and space (Banks & Riedl, 2022). In the United States, the National Institute of Standards and Technology, in Special Publication 800-53, defines a cyberattack as an intentional attempt to gain unauthorized access to, disrupt, destroy, or alter an information system, and considers critical infrastructure to include systems and assets whose failure would have a debilitating effect on national security, the economy, public health, or public safety (Banks & Riedl, 2022). In customary international law, Tallinn Manual 2.0, in Rule 92, defines a cyberattack as any cyber operation that is reasonably expected to cause death or injury to persons, or destruction of or significant damage to property (Schmitt, 2021). However, the United Nations, in the 2015 report of the Group of Governmental Experts, refrained from providing a precise definition of critical infrastructure and left the matter to the national sovereignty of states (Ghorbani, 2022). In this article, a cyberattack refers to any intentional and hostile act in cyberspace that, through intrusion into networks, information systems, or digital infrastructure, seeks to disrupt, destroy, or manipulate vital data and processes and produces adverse consequences for a country's national security, public health, economy, or social order. Critical infrastructure also refers to the set of physical and virtual facilities, systems, networks, and assets whose continuous functioning is essential for meeting the basic needs of society, preserving national security, and administering public affairs, and whose disruption would have catastrophic effects on public order (Crawford, 2013; Roscini, 2014).

The legal nature of cyberspace is another fundamental issue in determining the international responsibility of states. The basic question is whether cyberspace should be regarded as a "global commons" and a trans-territorial domain over which no state exercises sovereignty, or whether each part of cyberspace, because its physical infrastructure is located within the territory of a particular state, is subject to the sovereignty and jurisdiction of that state and forms part of its sovereign domain. At the early stage of the emergence of cyberspace, the theory of "cyber exceptionalism" held that cyberspace, due to its borderless and intangible nature, transcended the classical concepts of territory and sovereignty and required an independent legal system (Radsheld, 2022). Over time, however, the "sovereigntist" approach prevailed, and states realized that cyberspace relies on a physical substrate, all of which is located within the territorial domain of one or more states. Fiber-optic cables, data centers, and servers all have specific geographical locations and are therefore subject to the territorial sovereignty and jurisdiction of states (Banks & Riedl, 2022). The International Court of Justice, in the Nicaragua case and the Oil Platforms case, by emphasizing the principle of territorial sovereignty and the principle of non-intervention, provided a firm basis for applying these principles to cyberspace (Tsagourias, 2023). The United Nations also declared in the final 2021 report of the Group of Governmental Experts that state sovereignty and the norms arising from it apply to state conduct in cyberspace (Ghorbani, 2022). Nevertheless, some states and civil society institutions emphasize the need to formulate special rules compatible with the specific nature of cyberspace in order to strike a balance between the sovereign rights of states and the transboundary nature of cyberspace (Muller, 2024). In this article, in light of state practice and the position of the United Nations, cyberspace is regarded as a platform for the exercise of national sovereignty by states. This means that each state enjoys full sovereignty over the parts of cyberspace whose physical infrastructure is located within its territory, and any hostile act by another state against these parts constitutes a violation of sovereignty and intervention in domestic affairs (Sloan, 2023).

The foundations of the international responsibility of states in classical law constitute the main framework of this study. The international responsibility of states is one of the most fundamental concepts of public international law, according to which every state is held responsible for the breach of its international obligations and is required to make reparation for the damage caused. This concept reached its most developed form in the Draft Articles on Responsibility of States for Internationally Wrongful Acts, prepared by the International Law Commission in 2001. Although this draft is not a binding treaty, it is regarded as the most important instrument in this field and as reflecting customary rules of international law (Crawford, 2013). Under Article 1 of the Draft Articles, "every internationally wrongful act of a state entails the international responsibility of that state." Article 2 also sets out two essential elements for the establishment of responsibility: first, the conduct in question must be attributable to a state; and second, that conduct must constitute a breach of an international obligation of that state. These two elements, respectively referred to as "attribution" and "breach of obligation," constitute the main pillars of international responsibility (Mirabbasi, 2019). In classical law, the attribution of conduct to a state is based on specific criteria, primarily grounded in the concept of "control." Article 4 of the Draft Articles attributes the conduct of any state organ to the state, and Article 8 attributes to the state the conduct of persons or groups acting under the "direction or control" of that state (Zare, 2020). The consequences of responsibility are also explained in three categories of obligations: the obligation to cease the wrongful act, the obligation to offer assurances of non-repetition, and the obligation to make full reparation for the injury (Crawford, 2013). Despite this relatively comprehensive framework, classical law faces shortcomings in dealing with cyberattacks, the most important of which is the absence of specific rules for proving attribution in circumstances where a cyberattack is carried out through multiple servers and by non-state actors (Jackson, 2021). Nevertheless, many contemporary jurists argue that the general principles contained in the Draft Articles on State Responsibility, due to their flexibility and capacity for broad interpretation, can also be applied to cyberattacks through the application of the principle of dynamic interpretation (Goldman, 2022).

4. Elements Required for Establishing State Responsibility in Cyberattacks

The establishment of the international responsibility of states for cyberattacks against critical infrastructure depends on proving two essential elements, which are set out in Article 2 of the Draft Articles on State Responsibility prepared by the International Law Commission in 2001: first, "attribution," according to which the conduct in question must be attributable to

a specific state; and second, "breach of an international obligation," according to which the attributed conduct must constitute a breach of a binding international obligation. Together, these two elements form the causal chain for the establishment of responsibility, and the absence of either one prevents responsibility from arising (Jafari, 2020).

The first element, namely the rule of attribution, has faced unprecedented complexities in the field of cyberattacks. Unlike tangible and physical acts, in which identifying the actor and attributing the act to a particular state, although difficult, is possible, cyberattacks, due to their invisible, transboundary, and identity-falsifying nature, have effectively turned the identification of the true source of an attack and the proof of its connection with a state into a major challenge. In classical international law, attribution is possible through two main routes: first, the conduct of state organs, which, under Article 4 of the Draft Articles, is directly attributable to the state; and second, the conduct of persons or groups acting under the direction or control of the state, as provided in Article 8 of the Draft Articles (Heidari, 2018). However, in cyberattacks, states often use indirect instruments and carry out attacks through independent hackers, cyber paramilitary groups, or servers located in third countries in order to minimize the possibility of formal attribution (Karami, 2019).

One of the most important challenges in attributing cyberattacks is the use of intermediary servers and the falsification of Internet addresses. Cyber attackers usually pass through multiple servers in different countries, making the tracing of the original source of the attack almost impossible. In addition, techniques such as the use of infected computers in third countries, or botnets, further complicate attribution. Under such circumstances, proving that a specific attack is attributable to a specific state requires a set of technical, intelligence, and judicial evidence that is rarely fully available (Rezazadeh, 2019). State practice has shown that the attribution of cyberattacks is often carried out through political declarations or reports by intelligence organizations and is rarely referred to international judicial bodies. This practice, known as "political attribution" or "intelligence attribution," has replaced "legal attribution" and has created serious challenges for establishing international responsibility (Farajnia, 2022).

The second element, namely breach of an international obligation, has also become open to interpretation in cyberattacks against critical infrastructure. Article 12 of the Draft Articles defines breach of obligation in simple terms: a breach of an international obligation occurs when a state refrains from an act that it is required to perform or performs an act from which it is required to refrain. In the field of cyberspace, the most important obligations that may be breached include the principle of non-intervention in the internal affairs of other states, according to which no state may intervene in the internal or external affairs of another state, and the principle of the prohibition of the use of force, which, under Article 2(4) of the United Nations Charter, prohibits all states from threatening or using force against the territorial integrity or political independence of other states (Crawford, 2013). However, the question arises whether cyberattacks that lead to widespread power outages, disruption of the banking system, or paralysis of a country's air transport network can constitute "use of force" within the meaning of the Charter. Many jurists believe that if the physical consequences of a cyberattack are equivalent to the consequences of a traditional armed attack, it may be classified as use of force (Brownlie, 2019). Nevertheless, this interpretation has not yet become a uniform practice (Henry, 2020).

In view of the above difficulties, the simultaneous establishment of these two elements in cyberattacks, particularly where non-state actors are involved, faces serious obstacles. Nevertheless, some contemporary jurists believe that, through the application of dynamic interpretation and the formulation of evidentiary standards appropriate to the nature of cyberspace, the general principles of responsibility contained in the 2001 Draft Articles can also be applied to cyberattacks. From this perspective, there is no need for a fundamental revision of these rules; rather, emphasis should be placed on developing special rules in the field of evidence and attribution (Philipps, 2021). In this article, the establishment of state responsibility in cyberattacks is based on proving both elements of attribution and breach of obligation, and in the following sections, each of these elements will be examined in greater depth in light of the specific challenges of cyberspace (Martinez, 2022).

5. Evidentiary Challenges and Standards of Proof in Cyberattacks

One of the most important obstacles to establishing the international responsibility of states for cyberattacks is the evidentiary challenge and the absence of clear standards for the admissibility of evidence before international courts and institutions. Unlike traditional disputes, in which tangible and physical evidence such as documents, witness testimony, and

material traces can be easily presented and examined, cyberattacks are characterized by intangibility, susceptibility to falsification, mutability, and geographical dispersion, all of which make the evidentiary process highly complex (Rezaei, 2020). Proving that a specific cyberattack was carried out by a particular state or under the support and direction of that state requires a set of technical, intelligence, and legal evidence that is rarely fully available and, even where it exists, its credibility and admissibility are constantly disputed (Hosseini, 2021).

The first and most important challenge in this field is the problem of identifying the source of the attack and tracing the identity of the attacker. Cyber attackers, by using advanced techniques such as passing through multiple servers in different countries, falsifying Internet Protocol addresses, exploiting infected computers in third countries through botnets, and using virtual private networks, effectively make it impossible to trace the original source of the attack. This issue, known as "deniability," is one of the most important obstacles to legal attribution and forces states to rely on circumstantial and indirect evidence rather than definitive evidence in identifying the actor responsible for the attack (Mohammadinejad, 2019). In this context, digital evidence such as digital signatures, malicious codes, network traffic patterns, and metadata, although useful in identifying the source of an attack, is always subject to doubt regarding its authenticity and reliability due to the possibility of falsification and alteration, and therefore requires verification by independent experts and credible international institutions (Vaezi, 2022).

The second major challenge is the absence of clear and uniform standards regarding the level of evidence required to prove attribution in cyberattacks. In domestic legal systems, specific evidentiary standards exist, such as "beyond a reasonable doubt" in criminal matters or "balance of probabilities" in civil matters. However, in international law, especially in the field of cyberspace, no such clear standards have been developed. Some jurists emphasize the need to use the "clear and convincing evidence" standard, which represents an intermediate level between the two aforementioned standards and is more compatible with the complex nature of cyberattacks. Others argue that, given the evidentiary difficulties in cyberspace, the "preponderance of indications" standard should be used, under which a set of indirect indications and evidence, in the absence of counter-evidence by the accused state, may serve as the basis for attribution (Ranjbar, 2020). These disagreements have, in practice, created uncertainty for international courts and institutions in adopting a uniform approach.

The third challenge concerns the role and status of digital evidence and international cooperation in detecting and proving cyberattacks. Digital evidence, due to its fluid and vulnerable nature, requires specialized procedures for collection, preservation, and presentation, and any error in this process may result in the evidence being rendered invalid. On the other hand, collecting such evidence often requires access to servers and network equipment located within the territory of other states, which creates tension with the principle of territorial sovereignty of states (Salari, 2021). Accordingly, international cooperation through bilateral or multilateral agreements, as well as through international institutions such as Interpol and the United Nations, is essential for facilitating access to evidence and the exchange of information. However, such cooperation is often slow and ineffective because of states' reluctance to disclose sensitive information (Brown, 2020). Therefore, some jurists have proposed the establishment of an independent international body with technical and supervisory powers to investigate cyberattacks and provide expert opinions on evidence, so that the evidentiary process may acquire greater coherence and credibility (Wilson, 2022).

6. Judicial and State Practice in Confronting Cyberattacks

An examination of judicial and state practice shows that no uniform and coherent practice has yet emerged in confronting cyberattacks against critical infrastructure, and states adopt different approaches depending on their national interests, technical capabilities, and political relations. The most important examples of these practices include the cyberattack on Iran's nuclear facilities, known as Stuxnet, Russian cyberattacks against Ukraine's infrastructure, and the practice of United Nations bodies in formulating rules of conduct (Khosravi, 2020).

The cyberattack on Iran's nuclear facilities in 2010, known as Stuxnet, is regarded as one of the most complex and controversial cyberattacks in history. This attack, which was carried out with the aim of disrupting Iran's nuclear program, penetrated uranium enrichment facilities and, by altering the speed of centrifuges, caused significant damage to the facilities. Despite widespread speculation that the attack was designed and implemented by the United States and the Israeli regime,

neither of these states formally accepted responsibility, and the possibility of establishing international responsibility was effectively eliminated (Taghizadeh, 2018). This incident showed that, in practice, states use the strategy of denial and silence instead of accepting responsibility, and this further complicates the proof of attribution (Naderi, 2021).

Russian cyberattacks against Ukraine's infrastructure, especially the attacks on the country's power grid in 2015 and 2016, constitute another example of state practice. These attacks, which led to widespread power outages in large areas of Ukraine, despite technical evidence indicating the use of tools and malicious codes associated with hacker groups linked to Russia, did not face a specific legal response from the international community, and Ukraine was unable to prove Russia's responsibility before international courts. This incident showed that even where considerable technical evidence exists, the absence of clear evidentiary standards and the unwillingness of states to accept responsibility create a serious obstacle to the establishment of international responsibility (Imani, 2019).

At the level of United Nations institutions, the Group of Governmental Experts on responsible state behavior in cyberspace and the Open-ended Working Group, despite years of effort, have been unable to draft a comprehensive and binding treaty. The reports of these groups in 2013, 2015, and 2021 have largely been limited to formulating a set of non-binding rules and cooperation-oriented recommendations that do not possess the necessary effectiveness in deterrence, attribution, and reparation. Nevertheless, these reports have been able to create a relative consensus on some basic principles, such as respect for sovereignty, non-intervention in internal affairs, and international cooperation, which may serve as a basis for developing binding rules in the future (Ghorbani, 2022). Overall, existing practice shows that, in order to establish the international responsibility of states in this field, in addition to the need to draft a comprehensive treaty, effective evidentiary standards and supervisory mechanisms must also be established so that legal attribution may replace political attribution (Edwards, 2021).

7. Legal Effects and Consequences Arising from the Establishment of Responsibility

If both elements of attribution and breach of an international obligation are established in cyberattacks, the international responsibility of the wrongdoing state arises and entails specific legal effects and consequences. These effects, which are set out in the Draft Articles on State Responsibility prepared by the International Law Commission in 2001, are mainly identifiable in three categories of obligations: the obligation to cease the wrongful act and provide assurances of non-repetition, the obligation to make reparation for the damage caused, and the possibility of adopting countermeasures by the injured state (Mohaddesi, 2020).

The first and most immediate consequence of responsibility is the obligation of the violating state to cease the wrongful act. Article 30 of the Draft Articles requires the violating state, where the wrongful act is continuing, to cease it immediately and to provide the necessary assurances of non-repetition. In the field of cyberattacks, this obligation may include stopping cyber operations, removing malware from infected networks, and closing intrusion routes. However, because of the intangible and concealed nature of cyberattacks, monitoring the full implementation of this obligation faces serious difficulties, and the violating state may easily refuse to provide genuine assurances (Moradi, 2019).

The second important consequence of responsibility is full reparation for the injury caused, as emphasized in Article 31 of the Draft Articles. Reparation in cyberattacks faces serious challenges because of the intangible nature of many forms of damage, such as data loss, violation of privacy, disruption of public services, and reputational harm. Unlike physical damage, which can be measured and calculated, damage arising from cyberattacks is often intangible and long-term, and determining the amount of compensation requires accurate and specialized expert assessment. Reparation may take three forms: restitution, where possible; financial compensation; and satisfaction, including formal apology. However, each of these methods also faces numerous practical obstacles (Zarepour, 2021).

The third consequence is the possibility of adopting countermeasures by the injured state, which is recognized in Article 49 of the Draft Articles. Countermeasures are measures that the injured state temporarily and proportionately takes, contrary to its obligations toward the violating state, in order to induce that state to comply with its obligations. In the field of cyberspace, such measures may include proportionate cyber responses, such as cutting off access, blocking network traffic, and even conducting limited cyberattacks. However, these measures must be temporary, proportionate to the damage suffered, and aimed at inducing the violating state to comply with its obligations, and they must not violate human rights, peremptory norms, or

humanitarian principles (Farahani, 2020). Despite these limitations, countermeasures in cyberspace, due to their ease of implementation and the difficulty of identifying their source, may lead to escalation of tensions and widespread retaliatory actions, thereby endangering international stability (Richardson, 2021).

8. Conclusion

The analysis conducted in this article shows that the international responsibility of states for cyberattacks against critical infrastructure, despite the consolidation of its general principles in classical international law, faces serious challenges and obstacles in practice. The findings of the study indicate that the most important obstacle to establishing this responsibility is the difficulty of proving the attribution of cyberattacks to states. The intangible and transboundary nature of cyberspace, the possibility of identity falsification, and the use by states of non-state actors and intermediary servers have, in practice, minimized the possibility of tracing and legal attribution. In practice, states rely on political and intelligence attribution instead of legal attribution, which lacks the necessary binding force and effectiveness.

In addition, the absence of clear and uniform standards for the level of evidence required to prove cyberattacks constitutes the second serious obstacle in this field. The absence of a specific standard for the admissibility of digital evidence, the lack of clarity regarding the credibility of indirect indications, and the absence of uniform judicial practice in this regard have created hesitation among international courts and institutions in issuing judicial decisions. Moreover, state practice in dealing with cyberattacks, particularly in the cases of Stuxnet and attacks on Ukraine's infrastructure, has shown that states often refrain from accepting responsibility and resort to the strategy of denial and silence, which further increases the obstacles to the establishment of responsibility.

On the other hand, breach of an international obligation, as the second element of responsibility, although theoretically applicable to cyberattacks, remains open to interpretation because of concepts such as "use of force" and "aggression" in cyberspace and the absence of transparent criteria for assessing the severity of effects. This has prevented states from reaching a clear consensus in this regard. Nevertheless, if both elements of attribution and breach of obligation are established, specific legal effects and consequences, such as cessation of the wrongful act, reparation, and countermeasures, may be applied, each of which faces its own specific implementation challenges.

9. Recommendations

In light of the findings of the study, the following recommendations are offered to remove existing obstacles and facilitate the establishment of the international responsibility of states for cyberattacks:

A) Recommendations at the International Level

1. A comprehensive and binding international treaty should be drafted in the field of cyberspace, specifically addressing the responsibility of states for cyberattacks against critical infrastructure and providing clear definitions of cyberattack, critical infrastructure, and evidentiary standards. This treaty may be drafted as an additional protocol to the Budapest Convention or as an independent instrument within the framework of the United Nations.
2. An independent and specialized international body should be established with technical, supervisory, and judicial powers to investigate cyberattacks, collect and analyze digital evidence, and provide expert opinions on the attribution of attacks to states. This body may be established under the auspices of the United Nations or as an independent international organization, and its reports should be binding on international courts and institutions.
3. Clear and uniform standards should be developed for the level of evidence required to prove cyberattacks, using the combined criterion of "clear and convincing evidence" together with circumstantial and indirect evidence, and specific criteria should also be established for validating digital evidence and determining the role of independent experts in this process.
4. International cooperation should be strengthened in the areas of information exchange, attack detection, and extradition of cybercriminals through the conclusion of bilateral and multilateral agreements, as well as the creation of confidence-building mechanisms among states to facilitate the attribution process and prevent political misuse.

B) Recommendations for the Islamic Republic of Iran

1. Comprehensive domestic laws compatible with international standards should be drafted in the field of cybersecurity and the protection of critical infrastructure against cyberattacks, with emphasis on establishing supervisory mechanisms and rapid-response systems for attacks.
2. Technical and specialized capabilities for identifying, tracing, and collecting digital evidence of cyberattacks should be enhanced, and specialized centers for responding to cyberattacks should be established at national and regional levels.
3. Active participation should be pursued in the processes of developing international rules in the field of cyberspace within the framework of the United Nations and other international institutions, and specific legal proposals and positions should be presented regarding state responsibility for cyberattacks, with the aim of protecting national interests and enhancing the country's cybersecurity.
4. Regional and transregional cooperation should be strengthened in the areas of information exchange and technical and judicial cooperation regarding cyberattacks, especially with neighboring countries and states exposed to similar threats, and regional networks should be established to confront cyberattacks and exchange experiences.
5. Specialized legal and technical personnel should be trained and empowered in the field of international cyber law, and specialized courses should be designed to familiarize them with evidentiary challenges, standards of proof, and international judicial practices related to cyberattacks.
6. A comprehensive database of cyberattacks carried out against the country's critical infrastructure should be established, and the related evidence and indications should be documented for use in domestic and international proceedings, as well as for submitting regular reports to international institutions concerning cyberattacks and breaches of international obligations by other states.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Banks, C., & Riedl, J. (2022). *Legal Requirements for Cybersecurity*. Oxford University Press.
Brown, R. (2020). International cooperation in cyber evidence collection. *Journal of International Law*, *45*(3), 112-135.
Brownlie, I. (2019). *Principles of Public International Law* (9th ed.). Oxford University Press.
Crawford, J. (2013). *State Responsibility: The General Part*. Cambridge University Press.
Dinstein, Y. (2017). *War, Aggression and Self-Defence* (6th ed.). Cambridge University Press.
Edwards, M. (2021). State practice in cyber operations. *International Law Review*, *38*(4), 201-225.
Farahani, M. (2020). Countermeasures in cyberspace. *International Law Journal*, *24*(3), 145-170.
Farajnia, S. (2022). Political and legal attribution in cyberspace. *Strategic Studies*, *21*(4), 103-128.
Ghorbani, M. (2022). Practice of United Nations bodies in the field of cyberspace. *United Nations and Law Journal*, *15*(4), 57-82.
Goldman, R. (2022). Dynamic interpretation in cyber law. *Yale Journal of International Law*, *47*(1), 78-105.
Heidari, A. (2018). Attribution of conduct of state organs in cyberspace. *Comparative Law*, *11*(2), 75-98.
Henry, P. (2020). Use of force in cyberspace. *British Yearbook of International Law*, *91*(1), 156-182.
Hosseini, S. (2021). Digital evidence and evidentiary challenges in cyber disputes. *Legal Journal*, *36*(4), 105-130.
Imani, M. (2019). Russian cyber attacks against Ukraine and challenges of international law. *Comparative Law Research*, *12*(4), 89-110.
Jackson, T. (2021). Attribution challenges in cyber operations. *American Journal of International Law*, *115*(3), 423-456.

Jafari, H. (2020). Elements of international responsibility of states in cyber attacks. *Scientific-Research Journal of Constitutional Law*, *17*(34), 41-62.
Karami, A. (2019). Use of indirect instruments in cyber attacks. *Law and Technology*, *6*(1), 35-58.
Khosravi, A. (2020). Judicial and state practice in cyber attacks. *Law of Nations Journal*, *20*(4), 63-86.
Martinez, L. (2022). State responsibility in the cyber domain. *European Journal of International Law*, *33*(2), 445-472.
Mirabbasi, S. B. (2019). *Public International Law*. Mizan.
Mohaddesi, A. (2020). Legal effects of the realization of responsibility in cyber attacks. *Public Law Journal*, *14*(2), 87-110.
Mohammadinejad, H. (2019). Plausible deniability in cyber attacks. *Legal Journal*, *32*(2), 73-96.
Moradi, A. (2019). Obligation to cease the wrongful act in cyberspace. *Legal Research*, *12*(3), 45-68.
Muller, K. (2024). Digital sovereignty and international law. *German Yearbook of International Law*, *67*(1), 89-116.
Naderi, M. (2021). The strategy of denial in state practice. *Cybersecurity Studies*, *7*(3), 99-124.
Philipps, R. (2021). Evidentiary standards in cyber attacks. *Stanford Journal of International Law*, *57*(2), 234-261.
Radsheld, C. (2022). *Cyber International Law*. Mizan.
Ranjbar, A. (2020). Evidentiary standards in international cyber law. *International Legal Journal*, *23*(4), 89-112.
Rezaei, A. (2020). Evidentiary challenges in cyber attacks. *Technology Law Quarterly*, *8*(2), 43-68.
Rezazadeh, M. (2019). Use of intermediary servers and attribution of cyber attacks. *Law and Information Technology*, *5*(3), 77-100.
Richardson, S. (2021). Countermeasures in cyberspace. *International & Comparative Law Quarterly*, *70*(3), 567-594.
Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford University Press.
Salari, M. (2021). International cooperation in discovering cyber evidence. *Law and Politics Journal*, *17*(3), 99-124.
Schmitt, M. N. (2021). Sovereignty in cyberspace. *International Law Studies*, *97*(1), 112-138.
Sloan, R. (2023). Cyber responsibility and sovereignty. *Columbia Journal of Transnational Law*, *61*(2), 178-205.
Taghizadeh, R. (2018). The Stuxnet cyber attack and international responsibility. *Legal Journal*, *29*(2), 45-70.
Tsagourias, N. (2023). *State Responsibility in Cyberspace*. Cambridge University Press.
Vaezi, A. (2022). Digital evidence and its validation. *Legal Research*, *20*(1), 105-130.
Wilson, T. (2022). Independent international body for cyber investigations. *Georgetown Law Journal*, *110*(4), 789-816.
Zare, M. (2020). Control and direction in attribution of conduct to states. *Public law*, *12*(1), 55-78.
Zarepour, N. (2021). Compensation for damage in cyber attacks. *Private Law Research*, *9*(2), 119-144.
Zemanek, K. (2018). State responsibility and cyber attacks. In *Max Planck Encyclopedia of Public International Law*. Oxford University Press.
Ziaei Bigdeli, M. R. (2019). *Public International Law*. Ganj-e Danesh.