E.ISSN: 2661-7404 Academic Journal of Legal and Political Researchs P.ISSN:2571-9971
Year: 2026 Vol : 10 No : 02 Page : 63 - 79



# Digital Sovereignty and International Conflict: The Role of Cyberspace in Contemporary Global Politics

**Djebrane Sofiane** *
University of Oran 2 Mohamed Ben Ahmed
Laboratory of Public Policy and Regional
Security in Algeria
djebrane.sofiane@univ-oran2.dz

**Received: 21- 07- 2026** **Accepted: 08- 08- 2026** **Published: 22- 09- 2026**

**Abstract:**

The absence of a binding international legal framework increases the risk that cyberspace will remain unregulated, dominated by the interests of major powers. Cyberspace has become a key domain in international relations, reflecting the rapid development of information technologies and global interconnectedness, while creating new opportunities for conflict and cyberattacks targeting critical infrastructure, government, financial, and electoral institutions. This study examines the application of international law principles in cyberspace, such as sovereignty, prohibition of the use of force, and non-interference, and evaluates the effectiveness of existing legal frameworks in holding states accountable. It also analyzes international instruments and notable incidents, including the attacks on Estonia, Operation Stuxnet, and the SolarWinds breach, to highlight legal and procedural challenges in regulating cyberspace.

**Keywords :** security, geopolitics, international law, state responsibility, cyberspace, sovereignty, human rights.

* **Corresponding author**

E.ISSN: 2661-7404 Academic Journal of Legal and Political Researchs P.ISSN:2571-9971
Year: 2026 Vol : 10 No : 02 Page : 63 - 79



**Introduction :**

Cyberspace has emerged as a critical domain within the contemporary international system, rivaling traditional spheres such as land, sea, air, and outer space in strategic significance. Rapid advancements in information and communication technologies have facilitated unprecedented global connectivity, yet they have simultaneously expanded the landscape of potential conflict, enabling new forms of cyber threats and subversive activities. The growing frequency and sophistication of cyberattacks—targeting critical infrastructure, governmental institutions, financial systems, and electoral processes—underscore the complexity of ensuring security and accountability in an environment often characterized by anonymity and difficulties of attribution.

This study aims to examine the applicability and effectiveness of public international law in regulating state behavior in cyberspace, with a particular focus on the concept of State responsibility for internationally wrongful acts. It seeks to analyze how existing legal principles—such as sovereignty, the prohibition of the use of force, and the principle of non-intervention—are interpreted and applied within the cyber domain.

The central research question is: how does international law define and regulate State responsibility for actions conducted in cyberspace? Sub-questions include whether existing legal frameworks are sufficient to attribute responsibility, and to what extent States recognize, interpret, and effectively apply these norms within the realm of cybersecurity.

The study is guided by several key hypotheses. First, it assumes that the current framework of public international law is, in principle, applicable to cyberspace but faces significant challenges in practical implementation, particularly regarding attribution and enforcement. Second, it hypothesizes that the ambiguity surrounding cyber operations limits the effectiveness of existing legal mechanisms in establishing State responsibility. Third, it posits that there is an ongoing evolution toward the development of new norms and cooperative mechanisms to enhance legal certainty and accountability in cyberspace.

Methodologically, the research adopts an analytical and doctrinal approach, relying on the examination of international legal texts, state practices, and relevant scholarly literature. It also incorporates a comparative dimension by assessing emerging international initiatives and frameworks aimed at clarifying legal norms governing cyberspace.

E.ISSN: 2661-7404 Academic Journal of Legal and Political Researchs P.ISSN:2571-9971
Year: 2026 Vol : 10 No : 02 Page : 63 - 79



## Section I: security challenges in international relations and the geopolitical environment

While digital technologies have substantially enhanced quality of life, they have simultaneously created new avenues for criminal exploitation. Cybercriminals increasingly rely on sophisticated techniques to bypass security systems, which necessitates continuous monitoring and the constant evolution of defensive strategies. In this context, the sustainable development of the digital society depends on a comprehensive and integrated approach that combines legislative reform, technological innovation, and user awareness. Such a multidimensional strategy is essential to build and maintain trust, thereby reinforcing the resilience and stability of cyberspace[1].

Achieving effective cybersecurity requires coordinated efforts at both national and international levels. This involves the development of comprehensive national cybersecurity strategies, strengthening cooperation between public institutions and private sector actors, establishing robust legal frameworks to combat cybercrime, enhancing incident response mechanisms, and promoting public awareness of cyber risks. Moreover, threats such as intellectual property theft, insider attacks, and the proliferation of malicious software directly erode trust and pose serious risks to the stability of economic and social systems[2]

Trust represents a cornerstone for the sustainability and expansion of e-commerce and online communication. Users increasingly expect organizations not only to demonstrate technical competence but also to assume responsibility for safeguarding personal data. Any breach of trust can significantly reduce consumer loyalty and may even threaten business continuity. Unlike traditional commercial interactions—where physical presence and tangible infrastructures help establish confidence—trust in virtual environments remains inherently fragile and highly vulnerable to disruption[3]

Furthermore, the digital environment has facilitated new forms of misconduct and violence. Cyberbullying, online harassment, and cyberstalking have become widespread phenomena, encompassing behaviors such as sending threatening messages, disseminating harmful or offensive content, publishing

[1] Joseph S Nye Jr., **The Future of Power**, PublicAffairs, 2011, p. 113.
[2] P.W. Singer, Allan Friedman, **Cybersecurity and Cyberwar: What Everyone Needs to Know**, Oxford University Press, 2014, p. 67.
[3] Castells Manuel, **The Rise of the Network Society**, Wiley-Blackwell, 2009, p. 142.

personal data without consent, identity theft, and unauthorized access to personal accounts. These acts can result in severe psychological and financial harm to victims. Despite their gravity, existing legal frameworks often lack the specificity and effectiveness required to deter and adequately sanction such offenses[4]

Advances in information and communication technologies (ICTs) have undeniably generated significant benefits, including enhanced communication, expanded entertainment opportunities, accelerated commercial transactions, and more efficient data exchange. However, these same advancements have introduced complex security challenges. Cybercrime has emerged as a global and systemic threat, affecting individuals, corporations, and states alike, while undermining economic stability, political integrity, and public trust in the digital environment[5].

Cyber conflicts occurring within cyberspace can escalate into physical or economic consequences, including severe damage to critical national infrastructure. Such large-scale and strategically oriented cyberattacks constitute a serious threat to national security, particularly due to their relatively low cost and the high level of anonymity they afford to perpetrators[6]

Despite ongoing efforts, many existing cyber defense mechanisms remain insufficiently effective, as they often fail to impose substantial costs on attackers, thereby enabling repeated attempts even after initial failures. In a hypothetical scenario where computer systems are completely isolated, cybersecurity management would be significantly simplified, relying primarily on preventive measures such as background verification. However, in reality, achieving an optimal balance between functionality, security, and performance remains a complex and unresolved challenge, making it impossible to fully protect systems against all forms of cyber threats[7].

The strategic complexity of cybersecurity is further intensified by the rapid evolution of the Internet and digital technologies, which makes it extremely difficult for organizations to continuously adapt to emerging threats. Over time, cyber attackers have diversified their tools and techniques to target a wide range of

[4] Wall David S., **Cybercrime: The Transformation of Crime in the Information Age**, Polity Press, 2nd Edition, 2024, p. 98.
[5] Brenner Susan W., **Cybercrime and the Law : Challenges, Issues, and Outcomes, Northeastern** University Press, 2010, p. 55.

[6] Libicki, Martin C., **Cyberdeterrence and Cyberwar**, RAND Corporation, 2009, p. 45.
[7] Anderson Ross, **Security Engineering : A Guide to Building Dependable Distributed Systems**, Wiley, 3rd Edition, 2020, p. 212.

operating systems, communication protocols, and applications, thereby expanding the attack surface and creating an increasingly complex defensive environment[8]

This asymmetry tends to favor malicious actors, highlighting the critical importance of strengthening cyber intelligence capabilities, developing innovative defense strategies, and adopting automated systems for threat detection and response. Such measures are essential to enhance resilience and mitigate the risks associated with contemporary cyber conflicts.[9]

## Section II: International law and cyberspace

States increasingly rely on established norms of public international law to regulate conduct in cyberspace. This growing reliance has prompted critical debates regarding the relevance and effectiveness of existing legal frameworks in addressing the distinctive challenges posed by digital interactions, cybersecurity threats, and the complexities of jurisdiction within an interconnected global environment[10].

### A) Cyberspace and Territorial Sovereignty:

Sovereignty is widely regarded as a fundamental attribute of statehood and constitutes a core principle underpinning international relations. However, the practical independence of smaller and less powerful states has often been constrained, primarily due to the political interests and strategic calculations of more powerful states. This dynamic became particularly evident in the late twentieth century and continues to persist in contemporary international relations[11].

Cyberspace is generally understood as a vast and interconnected virtual environment in which digital interactions and experiences take place[12], It can be conceptualized as an expansive online domain where individuals utilize computers and the Internet to communicate, exchange information, and engage in various

[8] larke Richard A., Knake Robert K., **Cyber Cyber War: The Next Threat to National Security and What to Do About It**, HarperCollins, 2010, p. 78.
[9] Kello Lucas, **The Virtual Weapon and International Order**, Yale University Press, 1st Edition, 2017, p. 133.
[10] Michael N. Schmitt, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, Cambridge University Press, 2nd Edition, 2017, p. 3.
[11] Krasner Stephen D., **Sovereignty: Organized Hypocrisy**, Princeton University Press, 1999, p. 42.
[12] Joseph S Nye Jr., op.cit., p. 115

activities. Unlike the physical world, cyberspace encompasses all interactions mediated through digital technologies.[13]

The term "cyberspace" is used to describe the entirety of activities and processes associated with the Internet and networked systems. Despite numerous attempts by scholars and policymakers to provide a precise definition, there remains no universally accepted conceptualization. A widely recognized approach characterizes cyberspace as consisting of three distinct layers: the physical layer, which includes infrastructure; the logical layer, which relates to software and protocols; and the data layer, which encompasses information and digital content.[14]

The International Organization for Standardization (ISO), particularly through the ISO/IEC 27032, conceptualizes cyberspace as a multifaceted environment arising from the interaction between individuals, software, and Internet-based services. This environment is enabled by technological devices and interconnected networks that possess a tangible, physical dimension. From this standpoint, cyberspace may be described as a virtual domain in which diverse information technology systems are collectively utilized by individuals engaged in digital activities computer networks. The primary objective of these interactions is to facilitate communication and enable the organization and execution of specific human activities.[15]

Cyberspace is further characterized by its capacity to enable rapid and anonymous exchanges of information, presenting both opportunities and risks depending on the context. A defining feature lies in the ability of users to conceal their identities, thereby creating conditions conducive to potential acts of aggression carried out with a perceived sense of impunity. Its heterogeneous and complex nature poses serious challenges for the regulation of behavior and the protection of rights and security. Importantly, cyberspace is shaped more by the social interactions it enables than by its underlying technical infrastructure. Although it encompasses a global population exceeding that of any single state, it lacks centralized governance and universally accepted norms, which complicates the enforcement of human rights protections.[16]

[13] Cyberspace Definition of cyberspace in US English by Oxford Dictionaries, on the following website: https://www.oxfordlearnersdictionaries.com/definition/english/cyberspace accessed on 30 october 2025 at 4:12 a.m.
[14] Tobanksy Lior, "Basic concepts in cyber warfare", Military and Strategic Affairs, Vol. 3, 2011, p.80.
[15] ISO 27032: Guidelines for cybersecurity management, ISO, published:1 September 2022, on the following website: https://www.dataguard.com/blog/iso-27032/ accessed on 30 october 2025 at 4:33 a.m.
[16] Koh H. Harold, "International Law in Cyberspace", Harvard International Law Journal, Vol 54, 2012, p.6

At the same time, the physical infrastructure supporting cyberspace is largely situated within the sovereign territories of states and thus falls under their jurisdiction. However, the interconnected nature of global information systems means that actions undertaken within one state can produce significant cross-border effects in others.[17]

A key characteristic of cyberspace is its ability to transcend national borders, despite efforts by certain states—such as China—to promote the concept of cyber sovereignty. Within this framework, sovereignty extends beyond physical infrastructure to include all online activities conducted within national territory, as well as individuals subject to state jurisdiction. It also encompasses control over information entering or circulating within the national digital space. Nevertheless, the interconnected and interoperable nature of cyberspace facilitates operations that may challenge or undermine these sovereign interests.[18]

The growing complexity of sovereignty in cyberspace presents significant obstacles to international cooperation and to the development of coherent legal norms and regulatory frameworks aimed at ensuring security, stability, and the protection of digital rights. These challenges suggest that the issue of sovereignty in the digital domain will require increased attention in the future, particularly to establish clearer regulations and more consistent interpretations.[19]

It is also essential to acknowledge the diversity of actors operating within cyberspace. Among these are state-sponsored groups, often referred to as “troll armies,” which employ false identities to engage in online discourse, disseminate propaganda, influence public opinion, and undermine opposition movements. Another category includes organized opinion-shaping groups, commonly described as “swarm stream teams,” which utilize aggressive strategies to spread viral content—especially videos—with the aim of influencing collective perceptions. Furthermore, emerging state practice suggests that actions affecting foreign computer systems may be interpreted as violations of territorial sovereignty.[20]

[17] Villeneuve Nart , "Barriers to Cooperation: An Analysis of the Origins of International Efforts to Protect Children Online" in Controlled: The Shaping of Power, Rights, and Rule in Cyberspace, MIT Press, 2010, p.57.
[18] Duggan Patrick, "Harnessing cyber-technology's human potential", Special Warfare: The Professional Bulletin of the John F. Kennedy Special Warfare Center and School, Vol. 28, Issue 4, 2015, p.14.
[19] DeNardis Laura, **The Global War for Internet Governance**, Yale University Press ,2014, p. 88.
[20] Rid Thomas, **Active Measures: The Secret History of Disinformation and Political Warfare**, Farrar, Straus and Giroux , 2020, p. 211

The principle of sovereignty remains a foundational rule of international law, denoting the exclusive authority of a state to regulate activities within its jurisdiction, including its information infrastructure. In principle, cyberspace is not excluded from the application of this doctrine, as states retain the right to govern and protect their digital systems. However, the practical exercise of sovereignty is significantly constrained by the borderless nature of the Internet, which complicates jurisdictional enforcement when actions produce transnational effects on foreign systems.[21]

**B) Force in Cyberspace:**

Article 2(4) of the United Nations Charter establishes a general prohibition on the use of force in international relations, forming a cornerstone of the contemporary international legal order. However, the qualification of cyber operations as constituting a "use of force" remains a contested and unresolved issue within international law.[22]

In situations where cyberattacks produce consequences comparable to those of kinetic operations—such as significant physical destruction, the disruption of essential services (including hospitals or power generation facilities), or even loss of human life—there is a growing consensus among legal scholars and experts that such acts may fall within the scope of the prohibition on the use of force.[23]

Nevertheless, the majority of cyber operations do not reach this threshold of severity, which gives rise to substantial legal ambiguity regarding their classification. This uncertainty complicates the application of existing legal norms and raises important interpretative challenges for states and international institutions alike.[24]

Furthermore, cyber operations targeting foreign computer systems—particularly those that interfere with functionality or compromise data integrity—also raise critical questions concerning potential violations of territorial sovereignty. These issues highlight the need for clearer legal standards and more

[21] Schmitt Michael, op.cit., p. 15.

[22] United Nations Charter, 1945, p. 4.
[23] Michael Schmitt, op.cit., p. 330
[24] Tsagourias Nicholas, "Cyber Attacks, Self-Defence and the Problem of Attribution," Journal of Conflict and Security Law, Vol 17, Issue 2, 2012, p. 230

consistent state practice in order to determine when cyber activities cross the threshold into unlawful uses of force under international law.[25]

### C) States and the right to interfere in internal affairs in the cyber environment

Under international law, states have no right to interfere in the internal affairs of other states, in particular in the political, economic and social systems. Cyberattacks targeting electoral processes, public institutions or the media may constitute a violation of this principle.

Under applicable international law, a state may be held liable for cyberattacks if it is established that state officials actively participated in such actions, as the activities of the legislative, executive and judicial authorities are considered acts of the state. A state is liable for the actions of non-state actors that result in harm to another state only when those actions can be attributed to the state itself. International law stipulates that a cyber-operation conducted by a non-state actor can be attributed to a state under certain conditions. These conditions include cases in which the cyber act is carried out by an individual or entity authorized by the state to exercise public authority, or when such actions disrupt the computer systems of another state, thereby violating its territorial sovereignty[26]

### D) Development of international law in cyberspace

At present, the most significant multilateral legal instrument addressing cybercrime is the Budapest Convention on Cybercrime. Rather than establishing preventive mechanisms, this convention primarily provides a procedural framework that facilitates international cooperation in investigation and prosecution following cyber incidents.[27]

In the absence of binding global treaties specifically regulating cyberspace, the Tallinn Manual and its updated version, Tallinn Manual 2.0, represent influential scholarly efforts to interpret how existing norms of international humanitarian law and public international law apply to cyber

[25] Dinstein Yoram, **War, Aggression and Self-Defence**, Cambridge University Press, 6th Edition, 2017, p. 102.

[26] International Law Commission, Draft Articles on the Law of Treaties, Art. 5, 1966, p.3

[27] Council of Europe Convention on Cybercrime, (The Budapest Convention) 23 November 2001, ETS, No. 185, p.3

operations. Although these documents lack binding legal force, they have significantly shaped academic discourse and diplomatic practices, serving as a reference point for legal analysis in the cyber domain.[28]

Nevertheless, states often demonstrate reluctance to strengthen accountability mechanisms in cyberspace, as such developments may constrain their strategic and operational flexibility. Consequently, despite the growing importance of these manuals, their application remains dependent on the willingness of states to adopt or disregard their principles in practice.[29]

At the multilateral level, the United Nations has sought to promote consensus through initiatives such as the Group of Governmental Experts (GGE), established in 2004, which affirmed in its 2013 and 2015 reports that the UN Charter fully applies to cyberspace. In parallel, the Open-Ended Working Group (OEWG) provides an inclusive platform for all member states to discuss norms of responsible state behavior and confidence-building measures, although progress has remained gradual due to geopolitical disagreements.[30]

In addition to global efforts, regional and bilateral initiatives have also emerged. The Budapest Convention laid the foundation for cooperation in combating cybercrime, while bilateral agreements—such as the 2015 understanding between the United States and China—reflect attempts to manage cyber relations, albeit often shaped by political considerations and limited durability.[31]

Furthermore, the UN General Assembly adopted key resolutions in 2018, notably Resolution 73/27 on developments in information and telecommunications in the context of international security, and Resolution 73/266 on promoting responsible state behavior in cyberspace. These resolutions underscore the growing recognition of cyberspace as a domain requiring coordinated international governance.[32]

[28] Tsagourias, Nicholas, op.cit., p. 210.
[29] Michael Schmitt, op.cit., p. 5
[30] United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Reports (2013, 2015), p. 7.
[31] Segal Adam, **The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age**, Gildan Audio and Blackstone Audio, 2017, p. 145.

[32] UN General Assembly Resolutions, Advancing responsible State behaviour in cyberspace in the context of international security , 73/266, 2019, p. 2.

Despite general agreement that international law applies to cyberspace, significant divisions persist among states regarding the interpretation of core principles. Western states tend to support the extension of existing legal norms (status quo approach), whereas countries such as China and Russia advocate for a new international convention on information security that would enhance state control over digital space.[33]

Ultimately, the evolution of international law in cyberspace remains closely linked to the willingness of states to harmonize their regulatory frameworks. The transnational nature of cybercrime, often involving non-state actors, presents additional challenges, including difficulties in attribution, evidence collection, data management, and the preservation of confidentiality during investigations. Addressing these issues is essential to strengthening international cooperation and ensuring effective governance in the digital era.[34]

## Section III: states and their responsibility

In the contemporary international environment, cyberattacks have increasingly become instruments for pursuing geopolitical objectives, where responsibility is frequently attributed to states, either directly or through proxy actors. Nevertheless, the question of state responsibility in cyberspace remains among the most debated issues within international law.[35]

### A) Legal Basis for Responsibility:

#### - ILC Draft Articles on State Responsibility (2001)

In 2001, the International Law Commission (ILC) adopted the Draft Articles on Responsibility of States for Internationally Wrongful Acts, which are generally considered applicable to conduct in cyberspace. According to these Articles, the responsibility of a state arises upon the fulfillment of two cumulative conditions: the existence of a breach of an international obligation, and the attribution of the act in question to the state.[36]

[33] DeNardis Laura, op.cit., p. 95
[34] Brenner Susan, op.cit., p. 120.
[35] Schmitt Michael N., op.cit., p. 78.
[36] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, 2001, p. 34.

Accordingly, a cyber operation may entail international responsibility where it violates established legal obligations—such as the principles of sovereignty or the prohibition of the use of force—and can be legally attributed to a specific state.[37]

**B) the problem of attribution**

A major challenge in addressing cyberattacks lies in identifying the state responsible for such operations. The inherent anonymity and technical complexity of cyber activities often make it difficult, or even impossible, to definitively prove that official actors of a particular state carried out an attack.[38]

Attribution can occur at several levels[39]:

1. Direct state responsibility – where national security actors themselves execute the attack.
2. Indirect responsibility – proxy actors – where hacker groups act with the support, direction, or consent of a state.
3. Lack of control – permission or negligence – where a state knows, or should know, about malicious activities emanating from its territory but fails to prevent them.

The Tallinn Manual 2.0 recognizes that cyber attribution should rely on available evidence, but notes that the strict standards used in conventional warfare cannot always be applied, leaving room for potential political manipulation.[40]

The trajectory of human rights in cyberspace depends on evolving legal frameworks and their interpretation by national and international authorities. For instance, the United Nations Security Council met on 22 May 2020 to discuss cybersecurity, emphasizing that cyberattacks pose serious human rights risks. Measures like government-imposed internet shutdowns or hacking dissidents' devices can result in significant human rights violations.[41]

[37] Crawford James, **State Responsibility: The General Part**, Cambridge University Press, 2013, p. 113.
[38] Schmitt Michael N., op.cit., p. 154.
[39] Ibid., p. 155.
[40] Ibid., p. 156.
[41] United Nations Security Council, Cybersecurity and Human Rights, Meeting Record, 22 May 2020, p. 3.

### C) Real-life examples and state responses

1. Estonia (2007) – The first large-scale cyberattack on a state, widely attributed to Russia but without official confirmation ; no legal sanctions were imposed.
2. Stuxnet (Iran, 2010) – A complex cyberattack on Iranian nuclear facilities, believed to involve the US and Israel, but without official acknowledgment.
3. SolarWinds attack (USA, 2020) – A highly sophisticated attack affecting multiple government agencies, attributed to Russia but lacking formal international legal proceedings.

In all cases, the absence of an institutionalized mechanism for determining and enforcing state responsibility is evident. Responses have relied primarily on diplomatic measures, counter-cyber operations, and economic sanctions rather than formal legal processes[42]

## Section IV: reactions of states from the aspect of regional security

There is no universal mechanism to sanction states for cyberattacks. In addition to bilateral responses, states sometimes attempt to establish norms of responsible behavior in cyberspace through multilateral initiatives. However, many states (e.g., China and Russia) reject Western standards and propose alternative "digital sovereignty" models, slowing international consensus.[43]

During the 20th century, China's White Papers on Defense – revised approximately every two years – emphasized accelerating military reforms and developing advanced military technologies to modernize armed forces and strengthen national security in response to evolving regional and global dynamics.[44] Less developed states face significant obstacles in countering cyber threats, including detecting incidents, identifying perpetrators, and ensuring legally sound and timely regulation. The absence of international legal continuity complicates efforts to establish a coherent global framework for cyber regulation.[45]

[42] Lindsay Jon R., Cybersecurity and State Responses: Case Studies, 2021, p. 42.
[43] Joseph S Nye Jr., op.cit., p. 88.
[44] Anthony H. Cordesman, China's New 2019 Defense White Paper An Open Strategic Challenge to the United States, But One Which Does Not Have to Lead to Conflict, Center for Strategic and International Studies, 2019, pp. 12–15.
[45] Michael Schmitt, op.cit., p. 164.

States increasingly adopt national protective measures instead of adhering to established international standards. For instance, Russia and China advocate centralized state control over cyberspace, whereas Western countries support decentralized governance, reflecting their political structures and corporate influence. This divergence leads to international disagreements over cyber incidents, response methodologies, and implications for improving legal frameworks. Information sharing is essential for developing international cybersecurity regulations, but national autonomy in addressing vulnerabilities can hinder comprehensive enforcement and identification of cybercriminals.[46]

Ongoing geopolitical tensions, particularly the Ukraine conflict, reduce the prospects for harmonizing global efforts against cyberattacks. Cyberattacks have evolved into forms of cyberwarfare designed to inflict maximum political, military, and economic damage, representing a distinct form of aggression beyond conventional weapons.[47]

Cyberspace plays a dual role: enabling human rights while serving as a platform for violations. Proposals have emerged advocating recognition of unrestricted Internet access as a fundamental human right, establishing digital human rights. However, xenophobia, racism, and discrimination proliferate in the digital realm, and states often lack the capacity to protect individuals, leading to violations of international obligations and potential state responsibility. The complexity of attributing wrongful acts, combined with the presence of independent actors and major powers' ambitions to control the Internet, complicates accountability. Achieving consensus on jurisdiction and sovereignty rules remains a major obstacle. Although the principle of due diligence could mitigate shortcomings, practical implementation in cyberspace faces significant challenges.[48]

Cyberspace has become integral to state institutions, businesses, and daily life but introduces hybrid threats. These attacks often involve coordinated groups using false identities to spread propaganda, manipulate opinions, and perform subversive activities. Critical infrastructure, including government databases, energy, finance, and telecommunications, is vulnerable to unauthorized access, system failures, or network congestion. Hybrid attacks are difficult to detect and attribute, giving perpetrators strategic advantages. Consequently, there is no common understanding of norms, thresholds for liability, or cyber due

[46] Lindsay Jon R., op.cit., p.p. 45-46
[47] Ibid., p. 47.
[48] United Nations, Developing Digital Human Rights Frameworks, 2020, p. 7.

diligence, and state liability frameworks must evolve to address these unique challenges.[49]

## Conclusion:

The future trajectory of international law will depend largely on its ability to regulate emerging technologies and ensure accountability, even in domains where boundaries are unclear and consequences are profound. The interactions among major powers, particularly the United States, China, and Russia, are shaping both the legal and political evolution of cyberspace. While Western nations favor the extension of existing norms (status quo approach), China and Russia pursue new regulatory frameworks under the principle of digital sovereignty, granting them greater control over information and Internet governance at the national level. This divergence contributes to the fragmentation of global cyber norms and complicates the development of a universal regulatory framework.

Although fundamental principles of international law—such as sovereignty, the prohibition of the use of force, non-interference in internal affairs, and accountability for wrongful acts—apply to cyberspace, they are often ignored or selectively interpreted in practice. Key challenges include the technical difficulties of attributing cyberattacks, political obstacles in imposing sanctions on key actors, and the lack of binding multilateral agreements governing state behavior in the digital realm.

Without broader international consensus on implementing and advancing cyber norms, cyberspace risks remaining a domain of "legal minimalism," dominated by power politics rather than the rule of law. As a reflection of international relations, cyberspace underscores that failure to strengthen legal frameworks within this sphere can undermine the integrity of international law more broadly. The contemporary international order faces the critical task of reconciling traditional public international law principles with the evolving domain of cyberspace. Cyberattacks threaten critical infrastructure, manipulate information, and can impact democratic processes in other nations, demonstrating that the digital environment is far from intangible and carries significant consequences for international stability, security, and state accountability.

[49] Joseph S Nye Jr., op.cit., p.p. 92-94

**1- Bibliography:**

**A- International Laws :**

- International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, 2001.
- International Law Commission, Draft Articles on the Law of Treaties, Art. 5, 1966
- UN General Assembly Resolutions, Advancing responsible State behaviour in cyberspace in the context of international security , 73/266, 2019.
- United Nations Charter, 1945.
- United Nations Security Council, Cybersecurity and Human Rights, Meeting Record, 22 May 2020

**B - Books:**

- Anderson Ross, Security Engineering : A Guide to Building Dependable Distributed Systems, Wiley, 3rd Edition, 2020.
- Brenner Susan W., Cybercrime and the Law : Challenges, Issues, and Outcomes, Northeastern University Press, 2010.
- Castells Manuel, The Rise of the Network Society, Wiley-Blackwell, 2009.
- Crawford James, State Responsibility: The General Part, Cambridge University Press, 2013.
- DeNardis Laura, The Global War for Internet Governance, Yale University Press ,2014.
- Dinstein Yoram, War, Aggression and Self-Defence, Cambridge University Press, 6th Edition, 2017.
- Joseph S Nye Jr., The Future of Power, PublicAffairs, 2011.
- Kello Lucas, The Virtual Weapon and International Order, Yale University Press, 1st Edition, 2017.
- Krasner Stephen D., Sovereignty: Organized Hypocrisy, Princeton University Press, 1999.
- larke Richard A., Knake Robert K., Cyber Cyber War: The Next Threat to National Security and What to Do About It, HarperCollins, 2010.
- Libicki, Martin C., Cyberdeterrence and Cyberwar, RAND Corporation, 2009.
- Lindsay Jon R., Cybersecurity and State Responses: Case Studies, 2021.
- Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2nd Edition, 2017.
- Rid Thomas, Active Measures: The Secret History of Disinformation and Political Warfare, Farrar, Straus and Giroux , 2020.
- Schmitt Michael, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017, Cambridge University Press.
- Segal Adam, The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age, Gildan Audio and Blackstone Audio, 2017.
- Singer P.W., Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, 2014.
- Villeneuve Nart , "Barriers to Cooperation: An Analysis of the Origins of International Efforts to Protect Children Online" in Controlled: The Shaping of Power, Rights, and Rule in Cyberspace, MIT Press, 2010.
- Wall David S., Cybercrime: The Transformation of Crime in the Information Age, Polity Press, 2nd Edition, 2024.

**C -Newspaper articles:**

- Duggan Patrick, "Harnessing cyber-technology's human potential", Special Warfare: The Professional Bulletin of the John F. Kennedy Special Warfare Center and School, Vol. 28, Issue 4, 2015.
- Koh H. Harold, "International Law in Cyberspace", Harvard International Law Journal, Vol 54, 2012.
- Tobanksy Lior, "Basic concepts in cyber warfare", Military and Strategic Affairs, Vol. 3, 2011.
- Tsagourias Nicholas, "Cyber Attacks, Self-Defence and the Problem of Attribution," Journal of Conflict and Security Law, Volume 17, Issue 2, 2012.

**D- Rports :**

- Anthony H. Cordesman, China's New 2019 Defense White Paper An Open Strategic Challenge to the United States, But One Which Does Not Have to Lead to Conflict, Center for Strategic and International Studies, 2019.
- Council of Europe Convention on Cybercrime, (The Budapest Convention) 23 November 2001, ETS, No. 185.

**E- United Nations Reports :**

- United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Reports (2013, 2015).

**F- Websites:**

- Cyberspace Definition of cyberspace in US English by Oxford Dictionaries, on the following website: https://www.oxfordlearnersdictionaries.com/definition/english/cyberspace accessed on 30 october 2025 at 4:12 a.m.
- ISO 27032: Guidelines for cybersecurity management, ISO, published:1 September 2022, on the following website: https://www.dataguard.com/blog/iso-27032/ accessed on 30 october 2025 at 4:33 a.m.