Policy Journal of Social Science Review

Online ISSN 3006-4635

Print ISSN 3006-4627

Vol. 3 No. 5 (2025)

CYBERSECURITY AND SOVEREIGNTY: THE ROLE OF INTERNATIONAL LAW IN GOVERNING STATE BEHAVIOUR IN CYBERSPACE

[1]Seema Gul, [2]Wasmiya Malik, [3*]Gohar Masood Qureshi

[1]*Lecturer, Department of Law, University of Sialkot Pakistan*

[2]*MS Scholar International Islamic University, Islamabad, Pakistan*

[3*]*Lecturer, Department of Law, University of Sialkot, Sialkot, Punjab, Pakistan.*

[1]*gulseemao3@gmail.com*, [2]*wasmia.malik@gmail.com*

[3*]*goharqureshi2@gmail.com*

Abstract

The rapid digitization of state functions and global interconnectivity has elevated cyberspace into a critical domain of international relations, where issues of sovereignty and state conduct are increasingly contested. This research explores the extent to which international law governs state behavior in cyberspace, focusing on foundational principles such as sovereignty, non-intervention, and the prohibition of the use of force. The purpose of the study is to assess the adequacy of existing legal frameworks in addressing cyber threats and to identify gaps in accountability and enforcement. Employing doctrinal legal analysis and comparative review, the study evaluates key instruments including the UN Charter, customary international law, and the Tallinn Manual. The research finds that while international law provides a conceptual foundation, its application in cyberspace remains fragmented and underdeveloped, particularly in areas such as attribution, enforcement, and norm formalization. The study underscores the need for greater legal clarity, multilateral cooperation, and institutional mechanisms to strengthen international cyber governance while respecting digital sovereignty. These findings contribute to ongoing debates on how to balance national security interests with collective responsibility in maintaining a secure and open cyberspace as states increasingly rely on digital infrastructure, cyberspace has emerged as a critical domain for national security, economic stability, and political sovereignty. However, the inherently borderless nature of cyberspace poses complex challenges for the traditional principles of international law, particularly sovereignty, non-intervention, and the prohibition of the use of force. This article examines the evolving role of international law in governing state behavior in cyberspace, explores key legal principles, and assesses current efforts to develop a coherent framework for cybersecurity governance. It also evaluates the shortcomings of existing legal mechanisms and proposes pathways to enhance international cooperation and accountability in cyberspace.

Keywords: Digital sovereignty, Cyber norms, Attribution challenges, international accountability, State-sponsored cyber operations, Legal frameworks, Cross-border data governance, Due diligence obligations, Non-intervention principle, Critical infrastructure protection

Article Details:

Received on 15 April 2025

Accepted on 13 May 2025

Published on 15 May 2025

Corresponding Authors*:

Policy Journal of Social Science Review

Online ISSN 3006-4635

Print ISSN 3006-4627

Vol. 3 No. 5 (2025)

INTRODUCTION

In an era dominated by digital interdependence and technological advancement, cyberspace has become a crucial domain for state interaction, governance, and conflict. With the proliferation of cyber operations ranging from espionage and surveillance to cyberattacks on critical infrastructure questions arise about how traditional legal concepts such as sovereignty and non-intervention apply in the digital realm. The purpose of this article is to examine how international law governs state behavior in cyberspace, assess its effectiveness, and identify legal and normative gaps in the current international framework. The scope of the research includes a critical analysis of legal instruments such as the UN Charter, customary international law, and non-binding instruments like the Tallinn Manual, with an emphasis on their interpretation and applicability to cyber incidents. Set against the backdrop of increasing geopolitical tensions, the article interrogates whether current legal norms are adequate to regulate cyber conduct or whether new frameworks are necessary (Adonis, 2020; Khan & Ximei, 2022). The central questions addressed include: To what extent does existing international law constrain or permit state behavior in cyberspace? What challenges exist in enforcing accountability for cyber operations? The article adopts a doctrinal methodology, analyzing case law, treaties, state practice, and scholarly commentary. The findings suggest that while international law provides a foundational structure, its fragmented application and enforcement limitations hinder effective regulation of cyberspace. The article proceeds by first examining the concept of sovereignty in digital contexts, then analyzing key legal principles governing cyber operations, followed by a discussion on normative development, enforcement challenges, and concluding with recommendations for future legal frameworks (Moynihan, 2021; Khan et al., 2022).

In an era defined by digital interdependence, cyberspace has become a contested domain where state and non-state actors pursue strategic, economic, and political objectives. From cyber espionage and intellectual property theft to disruptions of critical infrastructure and electoral interference, the scope and scale of state behavior in cyberspace have raised urgent questions about the applicability and adequacy of international legal norms. This article investigates the extent to which international law, particularly the principles enshrined in the UN Charter and customary international law, can regulate state conduct in cyberspace while respecting state sovereignty.

RESEARCH METHODOLOGY

The research methodology for this study primarily employs a doctrinal legal research approach, which focuses on the analysis of primary and secondary legal sources, including international treaties, conventions, customary international law, and scholarly articles, to examine the interplay between cybersecurity and sovereignty in international law. This approach allows for a detailed exploration of existing legal frameworks, state practice, and normative developments, offering insights into the challenges and opportunities in regulating cyberspace. Secondary sources, such as legal commentaries, reports from international organizations like the UN and EU, and the Tallinn Manual, were analyzed to understand the current state of cyber governance and the application of international legal principles in cyberspace. Additionally, case studies of notable cyber incidents, such as the 2007 Estonia cyberattack and the Sony Pictures hack, were used to illustrate the practical implications of these legal concepts. Through qualitative analysis of these legal materials, this study evaluates the effectiveness of existing frameworks and provides

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 3 No. 5 (2025)

recommendations for future legal developments in the field of cybersecurity and state sovereignty.

THE CONCEPT OF SOVEREIGNTY IN THE DIGITAL AGE

Sovereignty, traditionally understood as the supreme authority of a state over its territory and the right to conduct its internal affairs without external interference, is a cornerstone of the international legal order. However, the emergence of cyberspace a domain that transcends physical borders and is largely controlled by decentralized and private entities has disrupted classical conceptions of state sovereignty. In this evolving digital environment, the question arises: how can states assert sovereign control and protect their interests without violating the sovereignty of others? Cyberspace is characterized by its transnational infrastructure, distributed control, and anonymity. Unlike conventional domains land, sea, air, and space cyber operations can be launched without crossing physical borders, often through civilian infrastructure located in third-party states. This creates legal ambiguity about what constitutes a breach of sovereignty in cyberspace. Some states, notably the United Kingdom and the Netherlands, assert that any unauthorized cyber intrusion into government networks or critical infrastructure constitutes a violation of sovereignty. Others, including the United States, adopt a more cautious approach, avoiding definitive statements on whether all cyber intrusions are inherently sovereignty violations (Chatinakrob, 2024; Khan, 2022).

The International Court of Justice (ICJ), in cases such as *Corfu Channel* (1949) and *Nicaragua v. United States* (1986), reaffirmed that states are prohibited from interfering in the internal affairs of other states and must respect their territorial integrity. Applying these principles to cyberspace suggests that cyber operations disrupting state functions, stealing classified data, or disabling infrastructure could violate international law. However, without a universally accepted definition of cyber sovereignty, interpretations vary significantly. Adding to the complexity is the rise of the *"digital sovereignty"* movement, where states seek to assert greater control over data, digital infrastructure, and information flows within their jurisdiction. This includes data localization laws, content regulation, and national firewalls. While such measures are often justified on security or cultural grounds, critics argue that they may fragment the global internet and restrict the free flow of information, undermining the openness of cyberspace (Assaf & Moshnikov, 2020; Khan & Wu, 2021).

Furthermore, sovereignty in cyberspace intersects with the principle of due diligence, which obliges states to prevent their territory from being used for acts that cause harm to other states. In the cyber context, this would require states to monitor and address malicious activities originating from their networks a challenging task given the technical difficulties of detection, attribution, and enforcement. In sum, sovereignty in the digital age is no longer confined to physical borders but extends to the virtual realm. Yet, the lack of consensus on its scope and application in cyberspace hampers efforts to regulate state behavior effectively. A shared understanding of what constitutes a sovereignty breach in cyberspace is essential to building norms of responsible state conduct and ensuring stability in the digital domain (Mueller, 2020; Abdelrehim Hammad et al., 2021).

Sovereignty, a foundational principle of international law, traditionally refers to a state's supreme authority within its territory and its freedom from external interference. In the digital context, sovereignty faces two key challenges: extraterritorial cyber operations that bypass physical borders, and the global nature of digital infrastructure

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 3 No. 5 (2025)

controlled by multinational corporations. International jurisprudence, including the ICJ's *Nicaragua v. United States* and *Corfu Channel* cases, underscores that sovereignty entails both territorial integrity and political independence. Applying these principles to cyberspace implies that unauthorized intrusions such as state-sponsored hacking or malware deployment may constitute violations of sovereignty. Yet, consensus on what constitutes a *"cyber intrusion"* under international law remains elusive (Heller, 2021; Usman et al., 2021).

LEGAL FRAMEWORKS GOVERNING STATE BEHAVIOR IN CYBERSPACE

THE UN CHARTER AND THE USE OF FORCE

The UN Charter, adopted in 1945, remains the primary legal instrument governing the use of force in international relations. Article 2(4) of the Charter prohibits states from threatening or using force against the territorial integrity or political independence of any state. The only exceptions to this prohibition are acts of self-defense under Article 51 or actions authorized by the UN Security Council under Chapter VII. While the Charter was drafted in a pre-digital era, its principles have been invoked in efforts to regulate cyber operations particularly those that may cause physical damage or significant disruption. One of the central questions in the application of the Charter to cyberspace is whether cyber operations can amount to a *"use of force."* There is growing scholarly and state practice consensus that cyber operations resulting in death, injury, or significant physical destruction such as disabling a power grid or interfering with critical infrastructure may qualify as a use of force under Article 2(4). The 2007 cyberattacks on Estonia, the Stuxnet worm targeting Iran's nuclear program, and the 2015 attack on Ukraine's power grid have each raised questions about whether such acts cross the threshold of prohibited force (Schmitt, 2020; Khan et al., 2020).

The Tallinn Manual 2.0, a non-binding academic study developed by legal and technical experts, offers guidance on this issue. It proposes that a cyber operation constitutes a use of force when its scale and effects are comparable to those of kinetic military operations. Factors to be considered include the severity, immediacy, and directness of the consequences; the military character of the operation; and the degree of intrusion into another state's territory. While the Manual reflects informed opinion, its recommendations are not legally binding, and states remain divided on their interpretation. A further challenge lies in determining whether a cyber operation constitutes an *"armed attack,"* which would trigger the right of self-defense under Article 51. While all armed attacks are uses of force, not all uses of force rise to the level of an armed attack. In the cyber context, this distinction is even less clear. For example, the insertion of malware into a nuclear facility might constitute an armed attack, whereas cyber espionage or data theft even if extensive may not (Meyer, 2020; Khan et al., 2020).

Moreover, the principle of necessity and proportionality, which limits the scope of self-defense, further complicates the legal response to cyber threats. Attribution remains a major hurdle accurately identifying the source and intent of a cyberattack is technically and politically complex, and without reliable attribution, lawful responses under the Charter become tenuous. Despite these uncertainties, a few states have begun to incorporate cyber operations into their national defense doctrines, signalling a recognition that cyber threats can implicate the jus ad bellum framework. However, in the absence of treaty provisions or binding jurisprudence, the legal contours of the use of force in cyberspace remain unsettled, leading to ambiguity and potential misuse.

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 3 No. 5 (2025)

In conclusion, while the UN Charter provides a foundational framework for assessing the legality of cyber operations, its application in cyberspace requires contextual interpretation and evolving legal standards. Clarifying when cyber operations cross the threshold of prohibited force is essential for preserving international peace and preventing escalatory cycles in the digital domain. The UN Charter prohibits the threat or use of force against the territorial integrity or political independence of any state (Article 2(4)). However, it remains contested whether cyber operations can amount to a *"use of force."* Legal scholars and states disagree on thresholds for example, whether a cyberattack causing physical damage or death, such as a shutdown of a hospital system, qualifies. The Tallinn Manual 2.0, developed by the NATO Cooperative Cyber Defence Centre of Excellence, provides non-binding guidance on applying international law to cyber operations. It suggests that if a cyber operation has similar scale and effects to a kinetic attack, it may constitute a use of force or even an armed attack, thus triggering the right of self-defense under Article 51 (Lahmann, 2021; Khan et al., 2020).

NON-INTERVENTION PRINCIPLE

The principle of non-intervention is a well-established norm of customary international law, rooted in the sovereign equality of states. It prohibits coercive interference by one state in the internal or external affairs of another, particularly in matters within a state's domestic jurisdiction such as political, economic, or military decisions. This principle, reaffirmed by the International Court of Justice in *Nicaragua v. United States* (1986), has significant implications for state conduct in cyberspace, especially in light of the increasing use of digital tools to influence foreign political systems, destabilize governments, and disrupt public services. In the digital realm, cyber operations that target electoral processes, disseminate disinformation to incite unrest, or undermine public institutions may constitute prohibited interventions if they are coercive in nature. The key element distinguishing unlawful intervention from mere influence is coercion acts that compel a state to act in a manner it would not have chosen freely. For instance, hacking into electoral databases to alter voter registration, or conducting ransomware attacks on government agencies to force policy change, could be considered coercive interventions and thus breaches of international law (Shi & Xu, 2021; Kahn & Wu, 2020).

However, interpreting coercion in cyberspace is inherently challenging. Not all forms of digital interference clearly meet the coercion threshold. Influence operations, such as propaganda or psychological operations conducted through social media, may affect public opinion but do not necessarily coerce state authorities. This ambiguity complicates efforts to distinguish between legal and illegal conduct under the non-intervention principle. Another dimension involves state-sponsored disinformation campaigns and *"information warfare,"* where coordinated efforts by foreign actors aim to manipulate narratives, polarize societies, or erode trust in democratic institutions. While these actions may fall short of coercion under a strict legal interpretation, they can have destabilizing effects that mimic traditional forms of intervention, prompting calls for broader legal recognition of non-kinetic coercive acts (Lenong, 2020).

The Tallinn Manual 2.0 attempts to clarify the scope of the non-intervention principle in cyberspace. It concludes that a cyber operation constitutes unlawful intervention when it involves coercive interference in a state's inherently sovereign functions, such as conducting elections, maintaining public order, or formulating foreign policy. Still, due to the manual's non-binding nature and varying state practices, its influence remains normative rather than authoritative. States differ in their

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 3 No. 5 (2025)

interpretations and thresholds. For example, France and the Netherlands have explicitly recognized that certain cyber operations, even those without physical damage, may violate the principle of non-intervention. In contrast, other states adopt narrower interpretations, limiting intervention to actions causing tangible or direct harm (Bechara & Schuch, 2021).

In practice, enforcement of the non-intervention norm is weak. The anonymity and deniability of cyber operations, combined with the absence of clear enforcement mechanisms under international law, make it difficult to hold violators accountable. Moreover, geopolitical tensions often prevent consensus on attribution and legal qualification of cyber incidents, further undermining the principle's deterrent effect. while the non-intervention principle remains a cornerstone of international law, its application in cyberspace is fraught with conceptual and practical difficulties. Clarifying the notion of coercion in digital contexts and building consensus on the scope of protected sovereign functions are essential steps toward strengthening the norm and enhancing international stability. The principle of non-intervention prohibits coercive interference in the internal affairs of another state. This principle could encompass cyber operations aimed at manipulating elections, inciting unrest, or disrupting governmental functions. However, establishing the coercive nature and intent of such operations pose's significant evidentiary challenges (Tsagourias, 2021).

CUSTOMARY INTERNATIONAL LAW AND DUE DILIGENCE

Customary international law, developed through consistent state practice accompanied by opinio juris (the belief that such practice is legally required), plays a significant role in filling normative gaps where treaty law remains silent particularly in the regulation of cyberspace. In the absence of a dedicated international treaty on cyber conduct, customary norms offer a foundational framework through which legal obligations and state responsibilities can be assessed. One such emerging norm is the duty of due diligence, which has attracted growing attention in cyber law discourse. Due diligence requires that a state must not knowingly allow its territory or infrastructure to be used in a manner that causes significant harm to the rights of other states. This principle was articulated in cases such as the *Trail Smelter Arbitration* (1941), where it was held that a state bears responsibility if harmful activities within its jurisdiction cause transboundary harm. In the cyber context, this translates into a duty for states to take reasonable steps to prevent, detect, and respond to malicious cyber operations emanating from their networks when those operations adversely affect other states (Broeders & Van Den Berg, 2020).

Although widely discussed, the precise contours of cyber due diligence remain underdeveloped in practice. For example, there is no universal agreement on what level of knowledge or control a state must have over non-state actors operating within its digital borders to trigger legal responsibility. Moreover, what constitutes a *"reasonable effort"* in monitoring or mitigating such activities in cyberspace where attribution and control are technically complex is contested. The Tallinn Manual 2.0 acknowledges the applicability of due diligence in cyberspace, stating that a state is internationally responsible if it fails to take appropriate steps to stop cyber operations launched from its territory once it becomes aware of them and they are causing serious adverse consequences to another state. However, this remains a soft law recommendation rather than a binding rule, and many states have yet to formally accept or operationalize it within their national frameworks (Ijaz, 2024).

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 3 No. 5 (2025)

Some states have begun articulating their own interpretations. For instance, France and Finland have issued national statements affirming the applicability of due diligence in cyberspace, while others like the United States remain more cautious, preferring strategic ambiguity. This divergence in state positions reveals the fragile consensus around the customary status of due diligence in cyberspace. Compounding the challenge is the lack of international mechanisms to verify compliance or resolve disputes over due diligence failures. In practice, many cyber operations attributed to state or non-state actors go unpunished, either due to the high threshold of proof required for attribution or due to political unwillingness to escalate matters diplomatically or militarily. This undermines the development of a robust due diligence norm and weakens the overall fabric of international cyber governance (Mainwaring, 2020).

Nevertheless, due diligence holds promise as a flexible and preventive tool that does not infringe upon sovereignty but instead reinforces responsible state behavior. Strengthening this norm through state declarations, regional frameworks, and international dialogues could enhance legal predictability and foster cooperation in addressing cross-border cyber threats. In conclusion, while due diligence is increasingly recognized as part of customary international law applicable to cyberspace, its practical implementation remains limited by technical, legal, and political challenges. Clarifying its thresholds and obligations is essential for the progressive development of international cyber law. States have a duty not to knowingly allow their territory to be used for acts that harm other states. In cyberspace, this translates into an obligation of due diligence states must prevent their cyber infrastructure from being used for cross-border cyber operations. Yet, enforcement mechanisms for due diligence are weak, and attribution remains a persistent obstacle (Haataja, 2022).

SOVEREIGNTY VS. CYBERSECURITY: TENSIONS AND DILEMMAS

The intersection of sovereignty and cybersecurity presents one of the most complex legal and strategic dilemmas in the digital age. On one hand, states assert their sovereign right to regulate, monitor, and defend digital activities within their jurisdiction. On the other, the inherently transnational nature of cyber threats enabled by borderless networks, encrypted communications, and global platforms demands a level of international cooperation that often clashes with unilateral assertions of digital sovereignty. One of the primary tensions arises when states prioritize cybersecurity through domestic control mechanisms that may infringe on the openness and universality of the internet. For instance, practices such as internet shutdowns, data localization mandates, and national firewalls while framed as sovereign acts to secure digital infrastructure can also suppress civil liberties, restrict global information flows, and fragment the internet into isolated digital spheres. These measures raise concerns about the balance between national security and the global public interest in maintaining an interoperable and open cyberspace (Ivanova et al., 2022).

Another layer of tension emerges in the context of foreign cyber operations. States often conduct surveillance, espionage, and even offensive cyber capabilities beyond their borders under the pretext of protecting national security. Yet these activities, when directed at another state's infrastructure or public institutions, may constitute violations of that state's sovereignty or the principle of non-intervention. Herein lies a core dilemma: how can a state defend itself against cyber threats that originate from beyond its borders without breaching the sovereign rights of others or triggering international conflict? The dilemma is further intensified by the challenges of attribution and asymmetry. States with

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 3 No. 5 (2025)

advanced cyber capabilities may engage in clandestine operations against less-developed nations, exploiting the latter's weak digital defenses without overt accountability. Conversely, smaller states or non-state actors may use asymmetric cyber tactics to target major powers. These dynamics lead to strategic mistrust and a race to develop cyber arsenals, undermining collective security (Raymond, 2021).

Efforts to resolve these tensions have been inconsistent. Initiatives like the UN Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) have sought to establish norms of responsible behavior in cyberspace, but consensus remains elusive particularly on issues such as the applicability of sovereignty, the regulation of offensive cyber capabilities, and the legitimacy of cross-border countermeasures. Private actors add another layer of complexity. Much of the internet's infrastructure is owned and operated by private entities, which may be subject to different legal regimes and corporate interests. States relying on these actors for cybersecurity can find their sovereignty constrained or diluted, particularly in cross-border data disputes or cybercrime investigations (Omar et al., 2022).

INTERNATIONAL COOPERATION AND NORM DEVELOPMENT

The rapid evolution of cyber threats has underscored the necessity for robust international cooperation and the development of norms to govern state behavior in cyberspace. Unlike traditional areas of international law, such as armed conflict or environmental protection, where states have established frameworks for cooperation, cyberspace presents unique challenges due to its borderless nature, the complexity of cyber threats, and the lack of universally accepted norms. The fragmented nature of current legal and policy frameworks means that states often act unilaterally or in small coalitions, which not only hampers effective cyber governance but also creates risks of escalating conflict in the digital domain.

INTERNATIONAL COOPERATION: THE CURRENT LANDSCAPE

International cooperation on cybersecurity has made some progress, but it remains inconsistent and often ad hoc. The UN has been at the forefront of fostering dialogue and developing norms to regulate state behavior in cyberspace. Key initiatives like the UN GGE and the OEWG have worked to establish principles for state conduct, emphasizing the need for responsible behavior, the protection of critical infrastructure, and the application of existing international law to cyberspace. The 2015 GGE report, for example, confirmed that the UN Charter, including principles of sovereignty and non-intervention, applies in cyberspace. It also recognized the need for states to take appropriate steps to prevent cyber incidents originating from their territory. However, the impact of these initiatives has been limited. While some states have adopted the recommendations, others, particularly those with advanced cyber capabilities, remain hesitant to accept binding agreements or international oversight of their cyber activities. States like the United States, China, and Russia continue to advocate for differing approaches based on their national security priorities, which creates significant divisions in the global cyber governance landscape (Dinh & Nguyen, 2024).

In the absence of a legally binding treaty, bilateral and regional arrangements have filled some gaps. For example, the European Union has made strides in cyber defense cooperation through the European Union Agency for Cybersecurity (ENISA) and the EU Cybersecurity Act, which sets out requirements for member states to enhance their cybersecurity capabilities and coordinate efforts to combat cyber threats. Similarly, the United States and its allies have established frameworks such as the NATO CCDCOE to

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 3 No. 5 (2025)

share information, conduct joint exercises, and develop cyber defense strategies (Krasikov & Lipkina, 2020).

NORM DEVELOPMENT: MOVING BEYOND SOFT LAW

Norm development in cyberspace remains largely in the realm of *"soft law"*non-binding agreements, declarations, and expert recommendations. The Tallinn Manual, while influential, is not a legally binding document, and states are not legally obligated to adopt its principles. However, it has played a crucial role in shaping discourse around cyber conduct, providing a common reference point for state practice and international debate. The challenge of norm development lies in reconciling differing views on sovereignty, the use of force, and the protection of privacy in cyberspace. States with authoritarian tendencies, such as Russia and China, have pushed for more restrictive norms that emphasize national control and limit the reach of international law. In contrast, liberal democracies advocate for an open, interoperable, and secure cyberspace governed by global norms of accountability, human rights, and freedom of expression. As states continue to develop their own cybersecurity strategies, the absence of universally accepted norms has led to a *"race to the bottom"* in certain cases. For instance, some states have employed offensive cyber tactics, such as deploying malware or engaging in cyber espionage, without facing significant international consequences. This lack of accountability has prompted calls for the establishment of clear international rules governing offensive cyber operations, attribution, and the use of cyber deterrence (Abdelkarim, 2024).

BUILDING A GLOBAL CYBER NORMATIVE FRAMEWORK

To strengthen international cooperation and norm development in cyberspace, several steps are necessary. First, greater political will is required to move from fragmented regional frameworks to a more cohesive global approach. A binding international treaty on cybersecurity despite its challenges could provide the necessary legal foundation to regulate state conduct, similar to other international treaties governing armed conflict or environmental protection. Second, the role of non-state actors, including multinational corporations and technical organizations, must be recognized in norm development. As private entities control much of the global internet infrastructure, their involvement in establishing norms for cybersecurity is crucial. Public-private partnerships can help ensure that legal frameworks account for both state interests and the operational realities of global digital systems (Khan et al., 2025).

Lastly, establishing clear mechanisms for accountability and dispute resolution is essential. This could include the creation of an international cyber court or an expansion of the role of existing institutions such as the ICJ in adjudicating state responsibility for cyber incidents. Additionally, frameworks for attribution that are widely accepted by the international community would help reduce ambiguity and deter malicious cyber operations while international cooperation and norm development in cyberspace have made strides, the road ahead is fraught with challenges. A more unified approach is needed, one that balances state sovereignty with collective cybersecurity, respects human rights, and promotes the safe and stable use of the digital domain. Only through sustained dialogue, transparent cooperation, and the gradual establishment of binding norms will the international community be able to address the growing threat of cyber insecurity while preserving the principles of sovereignty and peace (Khan & Ullah, 2024).

Efforts to develop norms of responsible state behavior have been spearheaded by the UN GGE and the OEWG. These bodies have achieved modest consensus on voluntary norms,

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 3 No. 5 (2025)

such as refraining from attacking critical infrastructure during peacetime and promoting capacity-building. Despite progress, such norms are politically—not legally—binding, and enforcement remains limited. Regional initiatives, such as the EU's Cyber Diplomacy Toolbox and ASEAN's cybersecurity cooperation, offer promising models but lack global applicability (Khan, 2024).

ACCOUNTABILITY, ATTRIBUTION, AND ENFORCEMENT CHALLENGES

One of the most significant hurdles in establishing effective international cybersecurity governance is the challenge of accountability, attribution, and enforcement. Unlike traditional military or diplomatic issues, where the responsible parties can often be identified with relative clarity, cyberspace presents unique complexities that undermine the ability to assign responsibility, hold perpetrators accountable, and implement enforcement mechanisms. The implications of these challenges are profound, particularly when states are the perpetrators or are accused of harboring non-state actors who launch cyberattacks (Khan, 2024).

Attribution—the process of identifying the responsible state or actor behind a cyberattack is one of the most elusive and controversial aspects of cybersecurity law. In the physical world, identifying the source of a military attack is often straightforward through conventional intelligence, satellite imagery, or diplomatic channels. In cyberspace, however, attacks can be launched anonymously or disguised using proxy servers, making it difficult to pinpoint the attacker with certainty. Many cyber operations are carried out through botnets, hijacked infrastructure, or encrypted communication channels, adding layers of complexity to the attribution process. This issue is not merely technical; it also involves significant political considerations, as states often face strategic incentives to deny or obfuscate their involvement in cyberattacks, even when evidence suggests otherwise. For example, during the 2007 cyberattacks on Estonia, many experts attributed the attacks to Russia, but Moscow consistently denied involvement. The lack of verifiable and universally accepted attribution mechanisms complicates international efforts to hold states accountable for hostile cyber activities. This challenge has prompted discussions within international legal forums, such as the UN GGE and the Tallinn Manual, which emphasize the need for more robust and transparent mechanisms of attribution, though these remain non-binding (Khan & Jiliani, 2023).

Once an attack is attributed, the next challenge is determining accountability. In traditional warfare, the concept of accountability is well established, with clear norms for state responsibility for the actions of their armed forces. However, in cyberspace, the lines between state and non-state actors are often blurred. States may either directly conduct cyber operations or indirectly support non-state actors, such as hacktivists or cybercriminals, who carry out attacks on their behalf. The principle of due diligence requires that states prevent harmful cyber activities emanating from their territory, but its application is complicated when dealing with actors over whom states may not have direct control or knowledge. The 2014 Sony Pictures hack, attributed to North Korean actors, raised questions about whether North Korea could be held accountable for activities carried out by non-state hackers, even if the state had supported or directed them. This issue is further complicated by the rise of state-sponsored cyber operations, which, while carried out by non-state actors, often have direct links to the state's political, military, or intelligence apparatus. International law has yet to establish clear standards for holding states responsible for cyberattacks launched by proxy actors, further undermining the deterrence effect (Khan & Usman, 2023).

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 3 No. 5 (2025)

Finally, enforcement of cybersecurity norms is hampered by a lack of established international legal mechanisms. In traditional international law, states have clear channels through which they can seek redress for violations of sovereignty, such as through diplomatic negotiations, the ICJ, or even collective security measures under the UN Charter. In cyberspace, however, these mechanisms are not fully adapted to address the unique nature of cyber operations. The decentralized nature of cyberspace means that the harms caused by cyberattacks are often difficult to quantify, making it challenging for states to prove that an attack has resulted in sufficient damage to warrant legal action or the use of countermeasures. Furthermore, even if attribution is established, states may be reluctant to take action due to political or strategic reasons. The absence of binding international legal agreements on cyberspace means that there is no global institution or tribunal capable of issuing enforceable rulings in cyber disputes. In practice, states often resort to retaliatory measures, such as offensive cyberattacks, sanctions, or economic pressure, rather than pursuing legal recourse through formal channels (Khan et al., 2023).

The increasing reliance on private sector actors for cybersecurity such as tech companies, internet service providers, and security firms means that enforcement may be further fragmented. These entities are often bound by national laws but not by international legal obligations, which complicates their role in cyber defense and governance. To address these challenges, international legal frameworks must evolve to better address issues of accountability, attribution, and enforcement in cyberspace. This may involve developing more reliable attribution mechanisms through international collaboration, establishing clearer norms of accountability, creating enforcement mechanisms such as binding treaties or international cyber courts, and promoting public-private partnerships to ensure that both states and non-state actors play their part in global cybersecurity governance. In conclusion, while progress has been made in addressing accountability, attribution, and enforcement in cyberspace, significant challenges remain. The evolving nature of cyber threats, the technical complexity of attribution, and the lack of universally agreed-upon legal standards make it difficult to develop effective mechanisms for managing state conduct in cyberspace. Addressing these challenges will require coordinated international efforts, legal innovation, and greater political will to build a secure, stable, and accountable cyberspace. A core difficulty in applying international law to cyberspace is attribution. Cyber operations are often conducted covertly, routed through multiple jurisdictions, and masked using sophisticated techniques. Without reliable attribution, holding states accountable under international law becomes difficult. Moreover, current international legal institutions lack the mandate or capacity to adjudicate cyber disputes. Calls for a specialized international cyber court or an independent attribution mechanism have emerged, but political will remains limited (Khan, 2023).

CONCLUSION

In conclusion, the relationship between cybersecurity and sovereignty presents one of the most pressing challenges in international law today. As cyberspace increasingly becomes a domain for both state and non-state actors to engage in political, economic, and military activities, states must navigate the delicate balance between asserting their sovereign rights and ensuring global cooperation to combat cross-border cyber threats. This research has explored the complexities of international law in governing state behavior in cyberspace, particularly focusing on issues of sovereignty, accountability, attribution, and enforcement.

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 3 No. 5 (2025)

One of the central findings of this study is that while there have been notable efforts to establish norms and frameworks for cyber governance, the lack of consensus among states remains a critical obstacle. International initiatives, such as those led by the UN and the development of documents like the Tallinn Manual, have been pivotal in guiding discourse, but they remain insufficient in terms of providing binding legal frameworks. The absence of universally accepted norms and the fragmentation of cyber governance structures have led to significant gaps in international law, leaving states vulnerable to cyber threats without clear mechanisms for redress. A key area for future research lies in the development of effective attribution mechanisms. As demonstrated, the difficulty of attributing cyberattacks accurately and definitively continues to impede accountability. Future research should explore how states, international organizations, and private entities can collaborate to build more transparent and technically advanced systems for cyber attribution that could foster greater trust and cooperation. Moreover, the legal implications of state-sponsored cyberattacks and the responsibilities of states in preventing attacks originating from their territories need further exploration, particularly in cases involving non-state actors and proxy warfare.

Another promising area for research is the creation of robust enforcement mechanisms in cyberspace. While traditional enforcement mechanisms like the ICJ have been effective in other domains of international law, they have proven ineffective in the cyber domain. Future studies should examine the feasibility of establishing an international cyber court or enhancing the role of existing bodies, such as the UN, in addressing disputes and imposing sanctions for violations of cybersecurity norms. Finally, the increasing involvement of private actors in cybersecurity governance presents both challenges and opportunities. Future research could explore the role of multinational corporations, tech giants, and international organizations in shaping global cybersecurity standards. Understanding how public-private partnerships can be leveraged to enhance cyber resilience, while balancing state sovereignty, is crucial for creating a secure and cooperative global cyber environment.

In sum, as the digital landscape continues to evolve, so too must the frameworks that govern state behavior in cyberspace. The future of international cybersecurity law hinges on the development of stronger legal norms, more effective attribution and enforcement mechanisms, and enhanced global cooperation. By addressing these gaps, the international community can pave the way for a safer, more secure cyberspace that respects both state sovereignty and collective security. The governance of cyberspace presents one of the most pressing legal challenges of the 21st century. International law offers foundational principles—sovereignty, non-intervention, and the prohibition on the use of force but their application to cyber operations is still evolving.To ensure a secure, stable, and equitable digital future, the international community must strengthen legal norms, foster cooperation, and build mechanisms for accountability that reflect the unique nature of cyberspace.

REFERENCES

Abdelkarim, Y. A. (2024). A literature review of the evolution of sovereignty and borders concepts in cyberspace. *International Cybersecurity Law Review*, *5*(2), 365-372.

Abdelrehim Hammad, A. A., Khan, A., & Soomro, N. E. (2021). Digital Economy Barriers to Trade Regulation Status, Challenges, and China's Response. *International Journal of Social Sciences Perspectives*, *8*(2), 41-49.

Adonis, A. A. (2020). International law on cyber security in the age of digital sovereignty. *E-International Relations*, *14*, 1-5.

Assaf, A., Moshnikov, D., (2020). International Law in the Digital Age'Research and Study Group Alaa Assaf Daniil Moshnikov. (2020). Contesting sovereignty in cyberspace. *International Cybersecurity Law Review*, *1*, 115-124.

Bechara, F. R., & Schuch, S. B. (2021). Cybersecurity and global regulatory challenges. *Journal of Financial Crime*, *28*(2), 359-374.

Broeders, D., & Van Den Berg, B. (Eds.). (2020). *Governing cyberspace: Behavior, power and diplomacy*. Rowman & Littlefield.

Chatinakrob, T. (2024). Interplay of International Law and Cyberspace: State Sovereignty Violation, Extraterritorial Effects, and the Paradigm of Cyber Sovereignty. *Chinese Journal of International Law*, *23*(1), 25-72.

Dinh, T. H., & Nguyen, P. C. (2024). Protecting National Sovereignty In Cyberspace Within The Context of Digital Globalization-Regulations of Some Countries And Proposals. *Eudaimonia-Journal for Legal, Political and Social Theory and Philosophy*, *8*(1), 5-29.

Haataja, S. (2022). Cyber operations against critical infrastructure under norms of responsible state behaviour and international law. *International Journal of Law and Information Technology*, *30*(4), 423-443.

Heller, K. J. (2021). In defense of pure sovereignty in cyberspace. *International Law Studies*, *97*(1), 50.

Ijaz, S. (2024). Cybersecurity and Sovereignty: The Conflict among States in Governing Cyberspace. *Pakistan Social Sciences Review*, *8*(4), 706-714.

Ivanova, K., Myltykbaev, M., & Shtodina, D. (2022). The concept of cyberspace in international law. *Law Enforcement Review*.

Kahn, A., & Wu, X. (2020). Impact of digital economy on intellectual property law. *J. Pol. & L.*, *13*, 117.

Khan, A. (2022). E-commerce Regulations in Emerging Era: The Role of WTO for Resolving the Complexities of Electronic Trade. *ASR Chiang Mai University Journal Of Social Sciences And Humanities*.

Khan, A. (2023). Rules on Digital Trade in the Light of WTO Agreements. *PhD Law Dissertation, School of Law, Zhengzhou University China*.

Khan, A. (2024). The Emergence of the Fourth Industrial Revolution and its Impact on International Trade. *ASR: CMU Journal of Social Sciences and Humanities (2024) Vol*, *11*.

Khan, A. (2024). The Intersection Of Artificial Intelligence And International Trade Laws: Challenges And Opportunities. *IIUMLJ*, *32*, 103.

Khan, A. S. I. F., Amjad, S. O. H. A. I. L., & Usman, M. U. H. A. M. M. A. D. (2020). The Evolution of Human Rights Law in the Age of Globalization. *Pakistan journal of law, analysis and wisdom*.

Khan, A., & Jiliani, M. A. H. S. (2023). Expanding The Boundaries Of Jurisprudence In The Era Of Technological Advancements. *IIUMLJ*, *31*, 393.

Khan, A., & Ullah, M. (2024). The Pakistan-China FTA: legal challenges and solutions for marine environmental protection. *Frontiers in Marine Science*, *11*, 1478669.

Khan, A., & Usman, M. (2023). The Effectiveness Of International Law: A Comparative Analysis. *International Journal of Contemporary Issues in Social Sciences*, *2*(3), 780-786.

Khan, A., & Wu, X. (2021). Bridging the Digital Divide in the Digital Economy with Reference to Intellectual Property. *Journal of Law and Political Sciences*, *28*(03), 256-263.

Khan, A., & Ximei, W. (2022). Digital economy and environmental sustainability: Do Information Communication and Technology (ICT) and economic complexity matter?. *International journal of environmental research and public health*, *19*(19), 12301.

Khan, A., Amjad, S., & Usman, M. (2020). The Role of Customary International Law in Contemporary International Relations. *International Review of Social Sciences*, *8*(08), 259-265.

Khan, A., Jillani, M. A. H. S., Ullah, M., & Khan, M. (2025). Regulatory strategies for combatting money laundering in the era of digital trade. *Journal of Money Laundering Control*, *28*(2), 408-423.

Khan, A., Usman, M., & Amjad, S. (2020). Enforcing Economic, Social, and Cultural Rights: A Global Imperative. *International Review of Social Sciences (IRSS)*, *8*(09).

Khan, A., Usman, M., & Amjad, S. (2023). The digital age legal revolution: taped's trailblazing influence. *International journal of contemporary issues in social sciences*, *2*(4), 524-535.

KHAN, M. I., Usman, M., KANWEL, S., & Khan, A. (2022). Digital Renaissance: Navigating the Intersection of the Digital Economy and WTO in the 21st Century Global Trade Landscape. *Asian Social Studies and Applied Research (ASSAR)*, *3*(2), 496-505.

Krasikov, D. V., & Lipkina, N. N. (2020, December). Sovereignty in Cyberspace: A Scholarly and Practical Discussion. In *XIV European-Asian Law Congress" The Value of Law"(EAC-LAW 2020)* (pp. 156-160). Atlantis Press.

Lahmann, H. (2021). On the politics and ideologies of the sovereignty discourse in cyberspace. *Duke J. Comp. & Int'l L.*, *32*, 61.

Lenong, J. (2020). State Cybersecurity Governance in the Fourth Industrial Revolution: An International Law Perspective. *The Disruptive Fourth Industrial Revolution: Technology, Society and Beyond*, 69-93.

Mainwaring, S. (2020). Always in control? Sovereign states in cyberspace. *European Journal of International Security*, *5*(2), 215-232.

Meyer, P. (2020). Norms of responsible state behaviour in cyberspace. *The ethics of cybersecurity*, 347-360.

Moynihan, H. (2021). The vital role of international law in the framework for responsible state behaviour in cyberspace. *Journal of Cyber Policy*, *6*(3), 394-410.

Mueller, M. L. (2020). Against sovereignty in cyberspace. *International studies review*, *22*(4), 779-801.

Omar, O. M., AlDajani, I. M., Juwaihan, M. E., & Leiner, M. (2022). Cybersecurity in sovereignty reform. In *Reconciliation, heritage and social inclusion in the Middle East and North Africa* (pp. 109-128). Cham: Springer International Publishing.

Raymond, M. (2021). Social Practices of Rule-Making for International Law in the Cyber Domain. *Journal of Global Security Studies*, *6*(2), ogz065.

Schmitt, M. (2020). Autonomous cyber capabilities and the international law of sovereignty and intervention. *International Law Studies*, *96*, 549-576.

Shi, J., & Xu, M. (2021). Visualizing international studies on cyberspace sovereignty: Concept, rationality, and legitimacy. *International Journal of Legal Discourse*, *6*(2), 251-289.

Policy Journal of Social Science Review

Online ISSN 3006-4635

Print ISSN 3006-4627

Vol. 3 No. 5 (2025)

Tsagourias, N. (2021). The legal status of cyberspace: sovereignty redux?. In *Research Handbook on International Law and Cyberspace* (pp. 9-31). Edward Elgar Publishing.

Usman, M. U. H. A. M. M. A. D., Khan, A. S. I. F., & Amjad, S. O. H. A. I. L. (2021). State Responsibility and International Law: Bridging the Gap.