Pinnacle in Social Sciences

January-June 2026, Vol. 01, No. 01, [37–42]
Published: 30st June 2026
Publisher: Pinnacle Research Company
https://ojs.pinnacleresearchcompany.com/index.php/PSS
RESEARCH PAPER

Sovereignty in Cyberspace: State Responsibility, Non-State Actors, and the Fragmentation of International Law

Soubia Qurban [1*] Fatima Wattoo [2] Sidra Naeem [3]

ABSTRACT

This research examines state sovereignty in cyberspace, focusing on state responsibility, non-state actors, and the fragmentation of international law. Using doctrinal analysis and case studies, it investigates challenges in attributing cyber operations, enforcing legal norms, and regulating transnational actors. Findings highlight the inadequacy of traditional sovereignty frameworks and call for multilateral, flexible legal mechanisms to ensure accountability and cybersecurity. The digital age has fundamentally challenged traditional notions of state sovereignty. Cyberspace, characterized by its borderless, decentralized, and rapidly evolving architecture, blurs conventional legal boundaries and complicates state responsibility. This article examines how international law currently addresses state obligations in cyberspace, the roles of non-state actors such as cybercriminals and private corporations, and the resultant fragmentation of legal norms. By analyzing case studies, state practice, and existing international frameworks, the paper argues that a reimagined legal framework is necessary to reconcile state sovereignty with the transnational realities of cyber operations.

Keywords: Cybersecurity, Digital Governance, Attribution, International Norms, Non-State Actors, Legal Fragmentation, Critical Infrastructure, State Accountability.

INTRODUCTION

The emergence of cyberspace has fundamentally transformed global interactions, challenging traditional concepts of sovereignty and state authority. Unlike physical territories, cyberspace is borderless, highly interconnected, and constantly evolving, enabling both state and non-state actors to operate with unprecedented speed and anonymity. These characteristics complicate the application of traditional international law, particularly regarding attribution,

[1] Visiting lecturer, international Islamic university Islamabad., Pakistan; sobia.qurban@gmail.com (**Corresponding)**
[2] lecturer, international Islamic university Islamabad.; fatimawattoophdscholor@gmail.com
[3] Vice principal Karakorum law college; sidranaeem99.sn@gmail.com

responsibility, and enforcement, raising urgent questions about how sovereignty can be effectively exercised in the digital domain. This research examines the legal implications of cyber operations, focusing on state responsibility, the influence of non-state actors, and the fragmentation of international legal norms. The study aims to evaluate the adequacy of existing frameworks in regulating cyberspace and to identify gaps that hinder accountability, security, and stability. The analysis is grounded in doctrinal research, reviewing legal instruments, state practice, and scholarly interpretations, and is supplemented by case studies of major cyber incidents to highlight practical challenges. The significance of this study lies in its potential to inform policymakers, legal scholars, and cybersecurity practitioners about the limitations of conventional sovereignty frameworks and the pressing need for adaptive legal solutions. It hypothesizes that state-centric legal approaches are insufficient for regulating transnational cyber activities and that non-state actors, including private companies, hacktivists, and cybercriminal networks, exacerbate the fragmentation of international law. Key questions addressed include how states can exercise sovereignty in cyberspace, what obligations arise from state responsibility, and what measures might harmonize fragmented norms. The study finds that ambiguity in attribution, the borderless nature of cyber operations, and the lack of universally accepted norms have weakened the effectiveness of international law in cyberspace. To address these challenges, multilateral cooperation, normative clarification, and flexible legal frameworks are essential. The article is organized to first conceptualize sovereignty in cyberspace, followed by an examination of state responsibility, the role of non-state actors, the fragmentation of international law, and finally, recommendations for developing a coherent legal framework for governing cyberspace. Sovereignty has historically been the cornerstone of international law, denoting the supreme authority of a state within its territorial borders. However, the rise of cyberspace an intangible, interconnected domain challenges the capacity of states to exercise traditional sovereignty. Cyber operations can originate from multiple jurisdictions simultaneously, involve non-state actors, and impact the essential functions of states without physical intrusion. This paper explores how these dynamics complicate the attribution of state responsibility, the enforcement of international law, and the protection of state sovereignty in the digital age (Tsagourias, 2016; Gul et al., 2025; Luidmila, 2021).

RESEARCH METHODOLOGY

This study adopts a qualitative methodology, analyzing primary and secondary legal sources to examine state sovereignty, responsibility, and non-state actors in cyberspace. Primary sources include international treaties, customary international law, UN GGE reports, and the Articles on State Responsibility, while secondary sources encompass scholarly articles, legal commentaries, and case studies of cyber incidents such as the Estonia 2007 attacks and Stuxnet. The research involves systematic identification, selection, and analysis of relevant legal instruments and state practice to evaluate existing frameworks, highlight gaps, and assess the applicability of international law to cyber operations. This approach allows for a comprehensive understanding of both theoretical principles and practical challenges, ensuring a rigorous and contextually grounded analysis of sovereignty and accountability in the digital domain.

CONCEPTUALIZING SOVEREIGNTY IN CYBERSPACE

Sovereignty in cyberspace requires a rethinking of traditional state-centric concepts that are rooted in territorial control. Unlike land, sea, or air, cyberspace is inherently borderless, allowing information and digital operations to flow across multiple jurisdictions instantaneously. This challenges the classical understanding of sovereignty as exclusive authority within defined territorial boundaries, forcing scholars and policymakers to consider sovereignty in functional and operational terms. In cyberspace, control is less about physical occupation and more about the capacity to regulate networks, protect critical infrastructure, and ensure the security of national digital assets. The complexity of cyberspace is further compounded by the multiplicity of actors operating within it. States no longer hold exclusive power over political, economic, and military activity in the digital domain. Private corporations, international organizations, hacktivist groups, and criminal networks play significant roles in shaping digital governance, often with global reach. These actors blur the lines of accountability and challenge states' ability to exercise exclusive control, creating a hybrid environment where sovereignty must coexist with shared responsibilities. Technological evolution also complicates the legal conceptualization of sovereignty. Emerging tools, such as cloud computing, artificial intelligence, and encryption technologies, allow cyber operations to bypass national defenses and obscure their origins, making attribution and enforcement difficult. Scholars have proposed understanding sovereignty in cyberspace as a "functional control" concept, emphasizing a state's ability to protect essential infrastructure, regulate harmful activity, and enforce domestic and international norms within its digital domain. This perspective balances traditional legal principles with the operational realities of a connected, decentralized cyberspace, suggesting that sovereignty is no longer purely territorial but also relational and capability-based (Chatinakrob, 2024; Gul et al., 2025; Assaf et al., 2020).

STATE RESPONSIBILITY AND CYBER OPERATIONS

State responsibility in cyberspace represents one of the most congested areas of international law, as traditional principles struggle to accommodate the unique characteristics of digital operations. Under customary international law and codified in the Articles on State Responsibility 2001, a state is liable for internationally wrongful acts committed by its organs or agents. However, applying these principles to cyber operations presents significant challenges, particularly when malicious acts originate from non-state actors using a state's territory or infrastructure. Attribution becomes a central issue, as determining whether a cyberattack is attributable to a state requires technical, legal, and evidentiary analysis, often complicated by anonymizing technologies and cross-border networks. States are also bound by a due diligence obligation, requiring them to prevent their territory from being used for activities that harm other states. In cyberspace, this principle raises complex questions about the extent of a state's responsibility to regulate private actors, including corporations, cybercriminals, or hacktivist groups, whose operations may indirectly support state objectives or undermine the security of other nations. The lack of universally accepted norms governing cyber conduct further complicates the enforcement of these obligations, leading to gaps in accountability and potential disputes between states. Notable cyber incidents illustrate these challenges in practice. For example, the 2007

cyberattacks on Estonia disrupted critical infrastructure, including banking, communications, and government systems. While technical evidence suggested links to actors within Russia, direct state involvement could not be conclusively established, highlighting the difficulty of attributing responsibility in cyberspace. Similarly, the 2010 Stuxnet operation targeting Iran's nuclear facilities demonstrated how sophisticated cyber operations could achieve strategic objectives without traditional military engagement, raising questions about proportionality, sovereignty, and the applicability of international law. These examples underscore the urgent need for legal frameworks that can address attribution, clarify state obligations, and provide mechanisms for accountability while maintaining flexibility to respond to the rapidly evolving cyber environment (Gul et al., 2025; Antonopoulos, 2021; Pierucci, 2025).

NON-STATE ACTORS AND LEGAL CHALLENGES

Non-state actors have become central players in cyberspace, challenging the traditional state-centric model of international law and complicating the enforcement of sovereignty. Hacktivist groups, cybercriminal networks, private cybersecurity firms, and even multinational corporations increasingly shape digital governance, often with capabilities that rival those of smaller states. Their activities can disrupt critical infrastructure, manipulate information, or conduct cyber espionage, raising questions about accountability and the applicability of existing legal norms. Unlike state actors, non-state actors operate across borders with relative impunity, exploiting jurisdictional gaps and inconsistent regulatory frameworks. The rise of hacktivism illustrates the difficulty of categorizing cyber operations under conventional legal frameworks. Politically motivated attacks, such as those carried out by Anonymous, blur the line between civil disobedience and acts that may constitute internationally wrongful conduct. Similarly, transnational cybercriminal organizations engage in theft, ransomware attacks, and financial fraud, causing extensive harm across multiple states. Private corporations, particularly those providing cybersecurity or offensive cyber capabilities, further complicate legal responsibility, as they may act as quasi-state actors without formal accountability mechanisms. The presence of these diverse actors highlights a critical legal challenge: traditional international law primarily governs state-to-state interactions, leaving non-state behaviour largely unregulated. Consequently, states may face pressure to respond to cyber incidents originating from actors outside their control, risking escalation or violation of international norms. This dynamic exacerbates the fragmentation of international law and underscores the urgent need for adaptive legal frameworks that can incorporate non-state actors into accountability structures while maintaining respect for state sovereignty (Eggenschwiler, 2020; Ahmed et al., 2025; Eslam & Tiwari, 2025).

CONCLUSION

The study of sovereignty in cyberspace demonstrates that traditional state-centric legal frameworks are increasingly inadequate in addressing the complexities of the digital domain. The borderless nature of cyberspace, the growing influence of non-state actors, and the difficulty of attributing cyber operations highlight significant gaps in existing international law. States face challenges in exercising effective sovereignty, enforcing accountability, and protecting critical infrastructure, while non-state actors exploit regulatory ambiguities to operate with limited oversight. This research underscores the need for a reimagined legal framework that balances state

authority with the realities of transnational cyber operations. Multilateral cooperation, normative clarity, and the integration of non-state actors into accountability mechanisms are essential to mitigate the risks of fragmentation and to maintain stability in cyberspace. Future research could explore the development of binding international agreements on cyber operations, mechanisms for cooperative attribution, and the role of emerging technologies, such as artificial intelligence, in shaping state and non-state responsibilities. Addressing these areas is critical not only for legal scholarship but also for policymakers and practitioners seeking to secure digital infrastructure and preserve the functional essence of sovereignty in the 21st century. Cyberspace represents both an opportunity and a challenge for international law. The traditional notion of sovereignty, grounded in territorial control, is inadequate to address the transnational, complex, and technologically mediated realities of the digital domain. States, while remaining primary actors, must engage with non-state actors and adapt legal norms to ensure accountability, security, and stability. A coherent, flexible, and multilateral legal framework is essential to mitigate the risks of fragmentation and preserve the functional essence of sovereignty in the digital age.

REFERENCES

Ahmed, F. A., Gul, S., & Shahzad, S. (2025). Ensuring accountability and transparency in AI-driven corporate governance. *International Journal of Social Sciences Bulletin*, *3*(5), 330-341.

Antonopoulos, C. (2021). State responsibility in cyberspace. In *Research handbook on international law and cyberspace* (pp. 113-129). Edward Elgar Publishing.

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.

Eggenschwiler, J. (2020). *Non-state actors and norms of responsible behaviour in cyberspace* (Doctoral dissertation, University of Oxford).

Gul, S., Ahmad, R., & Rahman, S. U. (2025). Constitutional dualities: Reconciling Islamic normativity with common law principles in hybrid legal systems. *Indus Journal of Social Sciences*, *3*(2), 674-693.

Gul, S., Malik, W., & Qureshi, G. M. (2025). Cybersecurity And Sovereignty: The Role Of International Law In Governing State Behaviour In Cyberspace. *Policy Journal of Social Science Review*, *3*(5), 121-135.

Gul, S., Saman, A., & Ahmad, F. (2025). The Convergence of Human Rights and Humanitarian Law: Recalibrating Legal Boundaries in Contemporary Conflict. *The Critical Review of Social Sciences Studies*, *3*(2), 1391-1403.

Tsagourias, N. (2016). Non-state actors, ungoverned spaces and international responsibility for cyber acts. *Journal of Conflict and Security Law*, *21*(3), 455-474

Luidmila, T. (2021). The issue of state sovereignty in cyberspace. *Legal Issues in the digital Age*, (2), 49-67.

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

Pierucci, F. (2025). Sovereignty in the digital era: Rethinking territoriality and governance in cyberspace. *Digital Society*, *4*(1), 27.

Eslam, H., & Tiwari, G. (2025). Cyberspace: Reimagining cybersecurity and its impact on state sovereignty. In *Cybercrime unveiled: Technologies for analysing legal complexity* (pp. 93-112). Cham: Springer Nature Switzerland