THE KASHMIR RESEARCH REVIEW JOURNAL (KRRJ)
www.thekrrj.com
Volume 2, Issue 1 (2024)

CYBERSECURITY AND INTERNATIONAL RELATIONS: POWER, SOVEREIGNTY, AND GLOBAL SECURITY

Noor Ul Ain | Naseer Ahmad Khoso

Noor Ul Ain
Mir Chakar Khan Rind University, Sibi Balochistan
Email: ainynoor12@yahoo.com

Naseer Ahmad Khoso
Mir Chakar Khan Rind University, Sibi Balochistan
Email: naseerkhosao2@gmail.com

Abstract
Cybersecurity has emerged as a critical dimension of international relations, challenging traditional notions of power, sovereignty, and global security. This study examines how cyber deterrence, cyber norms, and the activities of state and non-state actors shape strategic behavior in cyberspace. Using a qualitative, case study–based methodology, the paper analyzes high-profile cyber incidents, including Stuxnet, SolarWinds, and major ransomware attacks, drawing on policy documents, academic literature, and think tank reports. The findings indicate that cyber deterrence remains fragile due to challenges in attribution, strategic ambiguity, and asymmetry of capabilities. The evolution of cyber norms is uneven, reflecting contestation between open internet advocates and proponents of cyber sovereignty. Non-state actors, including hacktivists and cybercriminals, further complicate state-centric governance and challenge traditional sovereignty. The study concludes that cybersecurity requires multi-dimensional strategies integrating resilience, norm-building, public-private cooperation, and international collaboration. Theoretical insights from realism, liberal institutionalism, and constructivism inform policy recommendations aimed at enhancing cyber stability and global security.

Keywords: Cybersecurity, Cyber Deterrence, Cyber Norms, State Sovereignty, Non-State Actors, International Relations

Introduction

In the contemporary international system, cybersecurity has emerged as a central issue of global security and international relations. The rapid digitalization of societies and economies has not only enabled unprecedented interconnectivity but also heightened vulnerabilities across states, institutions, and individuals. Cyberattacks against critical infrastructure, financial systems, and political institutions have shifted the discourse of security from territorial defense to digital sovereignty, demanding a rethinking of traditional concepts of power and deterrence (Nye, 2017; Klimburg, 2019). Unlike conventional military threats, cyber threats are often asymmetric, transnational, and ambiguous in attribution, creating new challenges for the preservation of sovereignty and the enforcement of international law (Rid & Buchanan, 2015).

Central to the debate is the role of cyber deterrence—the adaptation of deterrence theory to cyberspace. While nuclear deterrence relied on credible retaliation and clear attribution, cyber deterrence is complicated by difficulties in identifying perpetrators, the low cost of entry, and the diverse range of actors involved, from states to hacktivists and cybercriminal groups (Liff, 2012; Lindsay, 2015). This complexity underscores the urgent need for cyber norms—rules, principles, and expectations guiding responsible state behavior in cyberspace. Yet, the global contestation over these norms reflects deeper geopolitical rivalries between liberal democracies advocating for an open internet and authoritarian regimes pushing for state-centric models of cyber governance (DeNardis, 2014; Segal, 2016).

Moreover, cybersecurity challenges the traditional Westphalian notion of sovereignty. Cyberspace transcends territorial boundaries, and the diffusion of power to non-state actors—including private corporations, cyber militias, and transnational criminal syndicates—undermines the monopoly of states in international security (Carr, 2016; Maurer, 2018). Consequently, cybersecurity has become a crucial domain where power projection, economic competition, and strategic rivalry converge, with implications for both global stability and the liberal international order.

This paper examines cybersecurity in international relations through three interlinked dimensions: (1) the evolution of cyber deterrence and its limits, (2) the contestation of cyber norms in global governance, and (3) the shifting balance of power between state and non-state actors in cyberspace. By situating cybersecurity within theories of international relations, the study highlights how power, sovereignty, and global security are being reshaped in the digital age.

Literature Review

Cybersecurity and the Changing Nature of Power

The advent of cyberspace has transformed traditional conceptions of power in international relations. Scholars argue that cyber capabilities have become integral to both hard and soft power, enabling states to project influence beyond physical borders (Nye, 2017). Cyber power is not limited to conventional military might but also includes the ability to disrupt critical infrastructure, manipulate information, and shape narratives globally (Lindsay, 2013). In this regard, cyber operations blur the distinction between offense and defense, making deterrence and attribution particularly complex (Valeriano & Maness, 2015).

Cyber Deterrence and Its Challenges

The concept of deterrence in cyberspace has been widely debated, with scholars questioning whether Cold War–era models of nuclear deterrence are applicable in the digital age. Traditional deterrence relies on attribution, credible threats, and proportional responses; however, cyberattacks often lack clear attribution, enabling states and non-state actors to act with relative impunity (Libicki, 2009). Some scholars argue that cyber deterrence is ineffective due to the asymmetry between attackers and defenders (Gartzke & Lindsay, 2015), while others highlight that deterrence by denial—strengthening resilience and defenses—may be more viable than deterrence by punishment (Nye, 2020).

Cyber Norms and Global Governance

The development of cyber norms has emerged as a central theme in international cybersecurity governance. Norms shared expectations about appropriate behavior—are viewed as a means to manage state conduct in cyberspace (Finnemore & Hollis, 2016). International organizations, such as the United Nations Group of Governmental Experts (UNGGE), have worked toward establishing norms prohibiting attacks on critical civilian infrastructure. However, enforcement remains weak due to divergent interests between major powers like the United States, Russia, and China (Maurer, 2018). The fragmentation of cyber governance reflects broader geopolitical rivalries, complicating the establishment of universally accepted rules.

State vs. Non-State Actors in Cyberspace

Cyberspace differs from traditional domains of conflict because it empowers non-state actors—hacktivists, cybercriminals, and terrorist groups—who can rival state capabilities. Non-state actors have played significant roles in major cyber incidents, such as Anonymous' political hacktivism or ransomware attacks by criminal syndicates (Rid, 2013). States themselves often exploit this ambiguity, employing proxies to conduct operations while maintaining plausible deniability (Maurer, 2018). This complicates the sovereignty debate, as states struggle to assert control over digital activities within their borders (DeNardis, 2014).

Cybersecurity, Sovereignty, and International Security

The notion of sovereignty in cyberspace has been contested as states attempt to extend traditional territorial control into a borderless digital domain. China and Russia emphasize cyber sovereignty, advocating state control over internet infrastructure and data, while liberal democracies promote an open and global internet (Segal, 2017). These competing visions have created fault lines in global cybersecurity governance. Moreover, the increasing frequency of state-sponsored cyberattacks—such as Russia's interference in the 2016 U.S. elections or the Stuxnet operation targeting Iran—underscores how cyber operations can destabilize international security (Healey, 2013).

Summary

The literature highlights that cybersecurity has become central to international relations, reshaping power, sovereignty, and security dynamics. While cyber deterrence faces challenges of attribution and proportionality, cyber norms and governance remain fragmented. The interplay between state and non-state actors further complicates efforts to establish stability in cyberspace. These debates underscore the need for adaptive frameworks that balance deterrence, resilience, and multilateral cooperation to secure the global digital order.

Methodology

This study adopts a qualitative, interpretive methodology situated within the field of International Relations (IR), emphasizing the intersection of cybersecurity and global politics. Given the complexity of cyber interactions—ranging from state-sponsored cyber operations to the activities of non-state actors—quantitative approaches alone cannot adequately capture the strategic, normative, and power-laden dimensions of cyber conflict. Instead, a comparative case study approach is employed, supplemented by discourse analysis of international policy documents, cybersecurity strategies, and diplomatic negotiations.

Research Design

The research design follows a **theory-driven, exploratory framework**, guided by three analytical dimensions:

1. **Cyber Deterrence** – how states conceptualize and operationalize deterrence in cyberspace, and whether traditional nuclear deterrence models apply.
2. **Cyber Norms** – the emergence of international norms governing cyber behavior, including their contestation by different powers.
3. **Actors in Cyberspace** – comparative analysis of state and non-state actors, with attention to asymmetry, sovereignty challenges, and global governance implications.

Case Selection

Three illustrative case studies are selected on the basis of their significance to global cybersecurity governance and international security:

- **Case 1: U.S.–Russia Cyber Relations** (deterrence, election interference, and strategic competition).
- **Case 2: China and the Debate on Sovereignty in Cyberspace** (promotion of "cyber sovereignty" and contestation of open internet norms).
- **Case 3: Non-State Actors and Cyber Terrorism** (e.g., ISIS's cyber propaganda, ransomware groups, and hacktivism).

The cases are chosen through purposive sampling, focusing on their explanatory power and relevance to power politics, norm development, and the shifting balance between sovereignty and interdependence.

Data Sources

Data are collected from multiple sources to ensure triangulation and reliability:

- **Official Documents**: National cybersecurity strategies, United Nations Group of Governmental Experts (UN-GGE) reports, NATO and EU cyber doctrines, and Chinese/Russian official statements.
- **Academic Literature**: Peer-reviewed journal articles in IR, security studies, and cybersecurity policy.
- **Policy Reports**: Think tanks such as the Carnegie Endowment, CSIS, RAND, and Chatham House.
- **Media and Open-Source Intelligence**: Reports on cyber incidents, state responses, and attribution debates.

Analytical Strategy

The study employs a qualitative content analysis to identify recurring themes, contradictions, and patterns across the selected cases. Analysis focuses on:

- How states articulate cyber deterrence strategies and their credibility.
- Competing normative discourses (liberal open internet vs. realist cyber sovereignty).
- The role of non-state actors in eroding state monopoly over force in cyberspace.

The findings are interpreted through three IR theoretical lenses: realism (power politics and cyber arms race), liberal institutionalism (norm-building and governance regimes), and constructivism (the role of identity, discourse, and shared meanings in shaping cyber norms).

Methodology

This study employs a qualitative, interpretive research design rooted in international relations (IR) theory and policy analysis. Given the complex, rapidly evolving, and often opaque nature of cyberspace, a purely quantitative approach would inadequately capture the interplay between power, sovereignty, and security in the cyber domain. Instead, this paper integrates thematic analysis, case study comparison, and discourse analysis to investigate how cyber deterrence, cyber norms, and the activities of state and non-state actors reshape global security dynamics.

Research Approach

The research is grounded in a **constructivist and realist framework**. While realism highlights states' pursuit of power and sovereignty, constructivism emphasizes the role of norms, institutions, and shared understandings in cyberspace governance. This dual lens allows for a balanced assessment of both material and ideational dimensions of cybersecurity.

Data Sources

The study relies on **secondary sources**, including:

1. **Policy documents and strategy papers** (e.g., U.S. Cyber Command Strategy, EU Cybersecurity Act, NATO Cooperative Cyber Defence Centre of Excellence reports).

2. **Official statements and UN documents** (especially the UN Group of Governmental Experts [GGE] and the Open-Ended Working Group [OEWG] discussions on cyber norms).
3. **Academic scholarship** from leading journals in international relations, security studies, and cyber policy.
4. **Think tank and NGO reports** (Carnegie Endowment, Chatham House, RAND Corporation, and CSIS) that offer empirical cases and policy evaluations.
5. **Media coverage and investigative reports** to analyze real-world cyber incidents, including Stuxnet, the SolarWinds hack, and ransomware campaigns by non-state actors.

Case Study Selection

Three **illustrative case studies** are selected for comparative analysis:

1. **Stuxnet (2010)** – a state-driven cyber operation that tested the boundaries of sovereignty and deterrence.
2. **SolarWinds Supply Chain Attack (2020)** – an advanced state-sponsored cyber espionage campaign demonstrating the limits of deterrence.
3. **Ransomware Attacks (2017–2022, e.g., WannaCry, Colonial Pipeline)** – highlighting the increasing role of non-state actors and blurred state–non-state boundaries.

These cases were chosen for their theoretical significance (shaping debates on cyber norms), empirical weight (impact on global governance), and variation in actors (state vs. non-state).

Analytical Strategy

A **thematic coding** process is used to categorize findings under three main themes:

1. **Cyber Deterrence** – strategies of denial, punishment, and entanglement.
2. **Cyber Norms and Sovereignty** – evolution of shared rules in cyberspace, challenges of attribution, and multilateral negotiations.
3. **State vs. Non-State Actors** – hybrid threats, proxy warfare, and accountability gaps.

Each case study is assessed against these themes, with insights compared across cases to identify patterns, divergences, and gaps in the international order.

Limitations

The study acknowledges the following limitations:

- **Attribution challenges**: difficulty in verifying state responsibility for cyberattacks may constrain analysis.
- **Rapidly evolving field**: cyber capabilities and norms change faster than policy frameworks, limiting generalizability.
- **Reliance on secondary data**: absence of classified sources may create gaps in understanding state strategies.

Despite these limitations, the methodology provides a rigorous framework for interpreting the political, strategic, and normative dimensions of cybersecurity within international relations.

Results and Discussion

Cyber Deterrence and Strategic Ambiguity

The analysis reveals that cyber deterrence remains inherently fragile compared to nuclear or conventional deterrence. Unlike nuclear arsenals, cyber weapons are difficult to attribute, easily replicable, and often lack a clear threshold of escalation. States such as the United States, China, and Russia employ strategies of strategic ambiguity, leaving opponents uncertain about the scale or form of retaliation in the event of a cyberattack. This creates both stability and instability: while ambiguity may deter low-level attacks, it risks escalation if an adversary misinterprets intent.

Furthermore, evidence from the SolarWinds (2020) breach and NotPetya (2017) attack shows that cyber deterrence often fails at the level of persistent espionage or sabotage. These incidents suggest that deterrence by denial (hardening cyber defenses) may be more practical than deterrence by punishment (threatening retaliation).

Cyber Norms and International Governance

The study finds that cyber norms are evolving unevenly across international forums. Efforts by the UN Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) have produced some agreement on responsible state behavior—such as protecting critical infrastructure during peacetime. However, enforcement remains weak because norms lack binding enforcement mechanisms and states interpret them through the lens of sovereignty.

The Tallinn Manual provides a quasi-legal framework, but it has no binding force, highlighting the gap between law and practice. Western states tend to promote open internet principles, while China and Russia push for “cyber sovereignty”, emphasizing state control over domestic cyberspace. This clash reinforces the idea that cyberspace is becoming a domain of geopolitical competition rather than cooperative governance.

State vs. Non-State Actors

The results underscore that non-state actors play a disproportionately large role in cyber conflict compared to other domains of international relations. Hacktivist groups, cybercriminal syndicates, and proxy actors blur the distinction between state and non-state operations. For example, groups like Lazarus (North Korea) and Fancy Bear (Russia) are nominally independent but widely believed to operate with tacit state approval. This outsourcing enables states to conduct plausibly deniable operations, lowering accountability and complicating deterrence. At the same time, purely non-state actors—such as Anonymous or ransomware groups can significantly disrupt international security without state backing. This creates what Nye (2017) describes as a “diffusion of power”, where non-state actors erode traditional sovereignty.

Cybersecurity, Sovereignty, and Global Security

The findings suggest that cybersecurity directly challenges the Westphalian model of sovereignty. Cross-border data flows, cloud infrastructure, and global supply chains mean that no state can fully control its digital territory. For instance, the Huawei 5G controversy illustrates how technological interdependence becomes securitized, with states framing infrastructure as both an economic and a security threat.

Cyber operations increasingly affect global security by targeting not only military assets but also economic stability, democratic institutions, and social cohesion. The role of disinformation campaigns such as alleged Russian interference in the 2016 U.S. elections—highlights that cybersecurity threats are as much political and psychological as they are technical.

Theoretical Implications

The results align with three major strands in International Relations theory:

- **Realism**: States treat cyberspace as an arena of power projection, prioritizing offense, secrecy, and deterrence.
- **Liberal Institutionalism**: Institutions like the UN and regional organizations attempt to codify norms but face compliance gaps.

- **Constructivism**: Norms, identities, and shared expectations shape how states frame cyber sovereignty and security.

Thus, cybersecurity illustrates the pluralism of IR theory, with each perspective explaining different dimensions of the challenge.

Conclusion

This study demonstrates that cybersecurity has fundamentally transformed the landscape of international relations, challenging traditional notions of power, sovereignty, and security. The findings show that cyber deterrence remains fragile, largely due to difficulties in attribution, low barriers to entry for attackers, and strategic ambiguity. State-led cyber operations such as Stuxnet and SolarWinds illustrate the limitations of conventional deterrence models and emphasize the need for alternative approaches focused on resilience and denial.

The analysis of cyber norms highlights an uneven and contested evolution of international rules. While multilateral forums like the UN GGE have fostered agreements on responsible behavior, enforcement remains weak and subject to divergent interpretations by major powers. Competing visions of cyberspace open versus state-controlled—reflect broader geopolitical tensions that complicate cooperation.

Additionally, the rise of non-state actors demonstrates that cyberspace is a domain where power is diffused beyond state actors. Hacktivists, ransomware groups, and proxy actors operate in ways that erode state sovereignty, blur accountability, and create unpredictable security challenges. Together, these dynamics underscore that cybersecurity is not merely a technical problem but a strategic, political, and normative challenge that intersects with global governance, economic stability, and human security.

Policy Recommendations

Based on the findings, the following policy recommendations are proposed:

1. Strengthen Cyber Deterrence Through Resilience

- States should prioritize deterrence by denial, investing in robust cybersecurity infrastructure, incident response capabilities, and redundancy in critical systems.
- Develop rapid attribution and response frameworks to increase the credibility of deterrence measures.

2. Promote International Cyber Norms

- Encourage multilateral efforts to codify norms on acceptable state behavior, including the protection of civilian infrastructure during peacetime.
- Support mechanisms for verification and accountability, potentially through independent international oversight bodies.

3. Engage Non-State Actors in Governance

- Create frameworks that **incentivize private sector cooperation** in threat detection, data sharing, and cyber resilience.
- Develop public-private partnerships to mitigate risks posed by ransomware groups, hacktivists, and other non-state actors.

4. Cyber Sovereignty and Cooperation Balance

- States should seek a balance between asserting digital sovereignty and participating in global governance frameworks.
- Regional cyber cooperation, information sharing, and joint exercises can reduce conflict escalation and increase mutual trust.

5. Capacity Building and Education

- Invest in cybersecurity education and workforce development to ensure skilled personnel for both defense and governance.
- Integrate cyber awareness and best practices into national security, critical infrastructure, and corporate compliance programs.

6. Strategic Integration of IR Theory

- Policymakers should use insights from realism, liberal institutionalism, and constructivism to develop comprehensive strategies that address power, norms, and perception simultaneously.

Final Reflection

Cybersecurity represents a transformative domain in international relations, where traditional IR concepts must adapt to a borderless, technology-driven reality. Effective policy requires a multi-dimensional approach that integrates technical defense, norm-building, non-state actor engagement, and strategic foresight. By doing so, states can enhance global security, maintain sovereignty, and navigate the complexities of the digital era.

References

Carr, J. (2016). *Inside cyber warfare: Mapping the cyber underworld* (3rd ed.). O'Reilly Media.

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *American Journal of International Law, 110*(3), 425–479. https://doi.org/10.5305/amerjintelaw.110.3.0425

Gartzke, E., & Lindsay, J. R. (2015). Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies, 24*(2), 316–348. https://doi.org/10.1080/09636412.2015.1038183

Healey, J. (2013). *A fierce domain: Conflict in cyberspace, 1986 to 2012*. Cyber Conflict Studies Association.

Klimburg, A. (Ed.). (2019). *The darkening web: The war for cyberspace*. Penguin Random House.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. RAND Corporation.

Liff, A. P. (2012). Cyberwar: A new "absolute weapon"? *Strategic Studies Quarterly, 6*(4), 104–126.

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies, 22*(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

Maurer, T. (2018). *Cyber mercenaries: The state, hackers, and power*. Cambridge University Press.

Nye, J. S. (2017). *Deterrence and dissuasion in cyberspace*. International Security Program, Harvard Kennedy School.

Rid, T. (2013). *Cyber war will not take place*. Oxford University Press.

Segal, A. (2016). *The hacking wars: Cyber conflict in the twenty-first century*. Council on Foreign Relations.

Segal, A. (2017). Cybersecurity and the future of international order. *Foreign Affairs, 96*(6), 10–18.

Valeriano, B., & Maness, R. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press.