

Governing Cyberspace in a Fragmented World: Regulatory Challenges and the Transformation of International Security Regimes

Ali Nazmi ÇORA*

ABSTRACT

This article examines the evolving complexities of cyber governance in the context of global order and international security regimes. As digital interconnectivity intensifies, cyber threats increasingly outpace traditional regulatory frameworks, generating normative, legal, and institutional challenges for international governance. Drawing on contemporary literature in international relations and cybersecurity studies, the study identifies key tensions between state sovereignty, multilateral regulatory efforts, and the informal nature of existing cyberspace governance structures. Findings indicate that the absence of binding international norms and the fragmentation of governance initiatives impede meaningful cooperation and accountability among states. Moreover, disparities in cyber capacity between developed and developing states amplify global inequalities while complicating collective security efforts. This research underscores the need for adaptive regulatory frameworks that integrate public-private partnerships, normative consensus, and capacity-building measures across regions. By advocating a multilayered approach that bridges legal reform and diplomatic norm creation, this paper contributes to ongoing debates on harmonizing cyber governance with broader international security objectives.

Key Words: Cyber governance, International security regimes, Global order, Regulatory challenges, International law.

JEL Classification: F50

Parçalanmış Bir Dünyada Siber Uzayın Yönetişi: Düzenleyici Zorluklar ve Uluslararası Güvenlik Rejimlerinin Dönüşümü

ÖZ

Bu makale, küresel düzen ve uluslararası güvenlik rejimleri bağlamında siber yönetişimin giderek karmaşıklaşan yapısını incelemektedir. Dijital karşılıklı bağımlılığın artmasıyla birlikte siber tehditler, geleneksel düzenleyici çerçevelerin kapasitesini aşmakta; bu durum uluslararası yönetim açısından normatif, hukuki ve kurumsal sorunlar doğurmaktadır. Uluslararası ilişkiler ve siber güvenlik alanındaki güncel literatüre dayanan çalışma, devlet egemenliği, çok taraflı düzenleyici girişimler ve mevcut siber uzay yönetim yapılarının büyük ölçüde enformel niteliği arasındaki temel gerilimleri ortaya koymaktadır. Bulgular, bağlayıcı uluslararası normların yokluğunun ve yönetişim girişimlerinin parçalı yapısının, devletler arasında anlamlı iş birliği ve hesap verebilirliği önemli ölçüde sınırlandırdığını göstermektedir. Bunun yanı sıra, gelişmiş ve gelişmekte olan ülkeler arasındaki siber kapasite farklılıkları, küresel eşitsizlikleri derinleştirirken kolektif güvenlik çabalarını da karmaşıklaştırmaktadır. Bu çalışma, kamu-özel sektör ortaklıklarını, normatif uzlaşmayı ve bölgesel kapasite geliştirme mekanizmalarını bütünleştiren uyarlanabilir düzenleyici çerçevelere duyulan ihtiyacı vurgulamaktadır. Hukuki reform ile diplomatik norm inşasını bir araya getiren çok

* Dr. Öğr. Üyesi, Onbeş Kasım Kıbrıs Üniversitesi, Siyasal ve Sosyal Bilimler Fakültesi, Uluslararası İlişkiler Bölümü, e-posta: alinazmicora@gmail.com, ORCID Bilgisi: 0000-0003-4159-0230

(Makale Gönderim Tarihi: 26.01.2026 / Yayına Kabul Tarihi: 01.09.2026)

Doi Number: 10.18657/yonveek.1872258

Makale Türü: Araştırma Makalesi

katmanlı bir yaklaşımı savunan bu makale, siber yönetişimin daha geniş uluslararası güvenlik hedefleriyle uyumlaştırılmasına ilişkin süregelen tartışmalara katkı sunmayı amaçlamaktadır.

Anahtar Kelimeler: *Siber yönetişim, Uluslararası güvenlik rejimleri, Küresel düzen, Düzenleyici zorluklar, Uluslararası hukuk.*

JEL Sınıflandırması: *F50*

INTRODUCTION

The rapid diffusion of digital technologies has fundamentally transformed the architecture of global order, reshaping how power is exercised, contested, and regulated in international politics. Cyberspace has emerged not merely as a technical domain, but as a strategic environment in which economic stability, political legitimacy, and national security increasingly intersect. Unlike traditional domains of the land, sea, air, and space, cyberspace is characterized by non-territoriality, anonymity, and high levels of private sector ownership, rendering conventional regulatory and security frameworks structurally inadequate (Deibert, 2019, pp. 23–29; Cavelti, 2014, pp. 701–705). As cyber operations now range from espionage and critical infrastructure disruption to election interference and influence campaigns, the governance of cyberspace has become a central concern for international security regimes. Yet, despite its growing strategic significance, cyber governance remains normatively underdeveloped and institutionally fragmented, posing profound challenges to the maintenance of global order (Nye, 2017, pp. 46–49; Choucri, 2012, pp. 3–8).

At the core of these challenges lies a fundamental tension between state sovereignty and the transnational nature of digital networks. International security regimes have historically relied on clearly demarcated jurisdictions, identifiable actors, and enforceable legal norms. Cyberspace, by contrast, blurs territorial boundaries and diffuses agency across state and non-state actors, including multinational corporations, criminal networks, and loosely affiliated hacker communities (Mueller, 2020, pp. 58–63). This diffusion complicates attribution, accountability, and deterrence—key pillars of traditional security governance. As a result, states increasingly struggle to reconcile their sovereign right to security with the practical necessity of international cooperation in cyberspace, producing a governance environment marked by strategic ambiguity and legal uncertainty (Kello, 2017, pp. 74–81).

Existing international efforts to regulate cyberspace have largely taken the form of voluntary norms, confidence-building measures, and expert-driven dialogues rather than binding legal instruments, reflecting political reluctance among major powers to accept formal treaty obligations in a domain where attribution and enforcement remain deeply contested (United Nations, 2021, pp. 7–11). Consequently, the emerging cyber governance landscape resembles a regime complex rather than a cohesive security regime, characterized by overlapping mandates, competing norms, and limited enforcement authority.

A further challenge concerns asymmetrical cyber capacity: advanced states possess the resources and expertise to shape global norms, while many developing states face structural constraints that limit their effective participation in governance

processes, undermining the inclusiveness and legitimacy of emerging regulatory arrangements (Madeline & Mueller, 2021, pp. 653–657).

Finally, the central role of private corporations in owning and operating critical digital infrastructure introduces additional regulatory complexity, as the absence of clearly defined legal responsibilities for private entities complicates accountability and coordination during cyber incidents (DeNardis, 2014, pp. 141–151).

Against this backdrop, this article argues that the regulatory challenges of cyber governance cannot be adequately addressed through incremental norm-building alone. Instead, they require a multilayered approach that integrates international law, diplomatic practice, institutional reform, and capacity-building mechanisms within a coherent security framework. The purpose of this study is to systematically analyze how normative, institutional, and legal dimensions of cyber governance interact to produce regulatory fragmentation within international security regimes. The study addresses the following research questions: (1) What are the principal regulatory challenges confronting cyber governance within international security regimes? (2) How do existing theoretical frameworks in international relations account for these challenges? (3) What governance approaches are most appropriate for addressing normative fragmentation, capacity asymmetries, and legal ambiguity in cyberspace?

The significance of this study lies in its integrative theoretical approach: by situating cyber governance simultaneously within realist, liberal institutionalist, and constructivist frameworks, it offers a theoretically grounded account of why existing regulatory arrangements remain inadequate and what conditions would be necessary for more effective governance. The scope of the study is global, encompassing state and non-state actors engaged in cyber governance processes, with particular attention to multilateral diplomatic forums, regional institutional arrangements, and public–private governance mechanisms. Regarding limitations, this study does not engage in primary empirical data collection or fieldwork; rather, it is based on a systematic qualitative literature review and comparative analytical synthesis of peer-reviewed scholarship, official policy documents, and international legal instruments. Accordingly, the findings are interpretive and analytical rather than statistically generalizable, and rapidly evolving technical developments in cyberspace may not be fully captured within the scope of the reviewed literature. By addressing these dimensions, the study aims to inform both scholarly debates and policy discussions on the future of international security in an increasingly digitalized world (Kello, 2017, pp. 201–207; Nye, 2017, pp. 61–64).

I. LITERATURE REVIEW

Scholarly engagement with cyber governance has expanded significantly over the past two decades, reflecting the growing recognition of cyberspace as a critical domain of international security. Early contributions to the field largely conceptualized cyberspace through technical or strategic lenses, emphasizing cyber threats as extensions of conventional military competition. However, more recent literature situates cyber governance within broader debates on global order, norm

formation, and regime theory in international relations. This shift underscores the inadequacy of state-centric security models when confronted with a domain characterized by transnational infrastructure, distributed agency, and rapid technological change (Kello, 2017, pp. 31–36). As a result, cyber governance is increasingly understood as a complex regulatory challenge that intersects with international law, institutional design, and global power asymmetries.

A prominent strand of the literature focuses on the absence of binding international legal frameworks governing state behavior in cyberspace. While international humanitarian law and the law of armed conflict provide foundational principles, their application to cyber operations remains contested. Scholars argue that ambiguity surrounding thresholds of use of force, attribution, and proportionality undermines legal certainty and weakens deterrence (Schmitt, 2017, pp. 19–27). This legal indeterminacy enables states to exploit gray zones below the threshold of armed conflict, thereby complicating efforts to regulate cyber behavior through existing security regimes. Consequently, cyber governance has evolved through informal norm-setting processes rather than formal treaties, raising questions about legitimacy, compliance, and enforcement (Nye, 2017, pp. 52–55).

Another influential body of literature examines cyber governance through the lens of regime complexity. Rather than a single, unified international regime, cyber governance consists of overlapping institutions, norms, and forums, including the United Nations, regional organizations, technical bodies, and private sector initiatives. Scholars argue that this fragmentation reflects both political disagreements among major powers and the structural characteristics of cyberspace itself (Mueller, 2020, pp. 71–78). While regime complexity can offer flexibility and innovation, it also generates coordination problems and normative inconsistency, particularly in the context of international security where clarity and predictability are essential (Betz & Stevens, 2013, pp. 94–99).

Norm development occupies a central place in the cyber governance literature. Diplomatic processes such as the United Nations Group of Governmental Experts (UN GGE) and the Open-Ended Working Group (OEWG) have been widely analyzed as key venues for articulating norms of responsible state behavior. Studies note that these forums have achieved limited consensus on principles such as state responsibility, due diligence, and the applicability of international law to cyberspace (United Nations, 2021, pp. 9–14). However, scholars also highlight persistent normative divides between Western states advocating an open, global internet and other actors emphasizing information sovereignty and state control (Tikk & Kerttunen, 2020, pp. 110–117). These divisions constrain the institutionalization of norms within formal security regimes.

Power asymmetry and inequality constitute another critical theme in the literature. Research on cyber capacity building demonstrates that states with advanced technological infrastructure wield disproportionate influence over norm-setting and regulatory agendas. Developing countries, by contrast, often lack the technical expertise, legal frameworks, and diplomatic resources necessary to engage effectively in cyber governance processes (Madeline & Mueller, 2021, pp. 655–

660). This imbalance not only marginalizes certain actors but also risks embedding existing global hierarchies into the emerging cyber order, thereby undermining claims of inclusivity and fairness in international security governance.

The role of non-state actors, particularly private technology firms, further complicates the cyber governance landscape. Unlike traditional security domains dominated by state authority, cyberspace is largely owned, operated, and innovated by private entities. Scholars emphasize that corporations such as internet service providers, cloud platforms, and cybersecurity firms exercise *de facto* regulatory power through technical standards and operational decisions (DeNardis, 2014, pp. 22–28). While public–private partnerships are increasingly promoted as governance solutions, the literature cautions that unclear accountability mechanisms and conflicting interests may dilute state authority and democratic oversight within international security regimes (Deibert, 2019, pp. 143–148).

A further strand of scholarship questions the very nature and severity of cyber conflict. Rid (2013, pp. 1–7) argues that cyber operations rarely meet the threshold of war and are better understood as forms of sabotage, espionage, or subversion, while Valeriano and Maness (2015, pp. 9–18) provide empirical evidence that most cyber disputes between states are restrained and do not escalate to armed conflict. These contributions usefully temper more alarmist accounts and underscore the importance of precise conceptual distinctions in governing cyber activities. Klimburg (2017, pp. 14–22) further highlights the dangers of cyber power being concentrated in the hands of both authoritarian states and unaccountable private actors, warning that the “darkening web” reflects a geopolitical struggle with profound implications for open governance. Cavelty (2014, pp. 703–707) argues that framing cybersecurity primarily through a national security lens creates its own risks, exacerbating the securitization of the internet in ways that may undermine civil liberties and open governance. Choucri (2012, pp. 11–18) situates cyber politics within the broader dynamics of international relations, showing how lateral pressure from state expansion into cyberspace generates new sources of conflict and governance demand. Carr (2016, pp. 44–50) examines the role of public–private partnerships in national cyber strategies, highlighting both their promise and the accountability deficits that arise when states delegate governance functions to private actors. Finally, emerging scholarship calls for integrative and adaptive governance models capable of bridging legal, diplomatic, and technical dimensions of cyberspace. Rather than pursuing comprehensive treaties, some scholars advocate incremental norm consolidation supported by confidence-building measures, regional initiatives, and capacity development programs (Kello, 2017, pp. 183–189; Healey, 2013, pp. 267–272). Others emphasize the importance of embedding cyber governance within broader discussions of global order, recognizing cyberspace as a constitutive element of contemporary international relations rather than a peripheral technical issue (Nye, 2017, pp. 61–64; Hansen & Nissenbaum, 2009, pp. 1157–1162). Collectively, this literature highlights both the progress made and the persistent challenges confronting cyber governance as a component of international security regimes.

II. METHODOLOGY

This study adopts a qualitative, interpretive research design to examine the regulatory challenges of cyber governance within international security regimes. Given the normative ambiguity, institutional fragmentation, and evolving nature of cyberspace, a qualitative approach is particularly appropriate for capturing the discursive, legal, and political dimensions that shape governance outcomes. Rather than seeking causal generalization, the study aims to generate analytical insight into how regulatory frameworks are constructed, contested, and operationalized in the international system (Creswell & Poth, 2018, pp. 42–47). This design aligns with interpretivist traditions in international relations that prioritize meaning, norms, and institutional practices over purely material indicators.

The study employs a systematic qualitative literature review, complemented by comparative legal and institutional analysis. The literature review follows a structured selection process designed to ensure analytical rigor and transparency. Peer-reviewed journal articles, academic monographs, and official policy documents were selected from established databases including Web of Science, Scopus, and JSTOR. Inclusion criteria required sources to address at least one of the following dimensions: cyber norms, international security regimes, governance mechanisms, or international law applicable to cyberspace. Foundational works in international relations theory and cybersecurity studies were prioritized to anchor the analysis in established scholarly debates (Booth, Colomb, & Williams, 2016, pp. 75–81).

To enhance analytical coherence, the study employs thematic coding as its principal analytical technique. Textual data were coded inductively to identify recurring concepts, arguments, and normative positions across the selected literature. Initial codes included categories such as sovereignty, norm formation, regime complexity, capacity asymmetry, and public–private governance. These codes were subsequently refined through iterative comparison to identify dominant patterns and points of contention within the literature (Saldaña, 2016, pp. 98–104). This process enables the systematic organization of complex debates and facilitates comparative assessment across legal, institutional, and political dimensions of cyber governance.

In addition to thematic coding, the study incorporates a comparative institutional analysis to evaluate how different governance forums address regulatory challenges in cyberspace. Particular attention is given to multilateral diplomatic processes, including United Nations–led initiatives, as well as regional and multi-stakeholder governance arrangements. By comparing formal and informal governance mechanisms, the study assesses their relative capacity to generate normative consensus, ensure compliance, and mitigate security risks (Karns, Mingst, & Stiles, 2015, pp. 42–48). This comparative perspective highlights the structural strengths and limitations of existing security regimes when applied to a non-territorial domain such as cyberspace.

The methodological framework is further informed by international regime theory, which provides conceptual tools for understanding how norms, rules, and

decision-making procedures emerge and function under conditions of anarchy. Regime theory is particularly well-suited to analyzing cyber governance, as it accommodates both formal institutions and informal arrangements that shape state behavior (Keohane, 1984, pp. 57–63). By applying this framework, the study situates cyber governance within broader debates on cooperation, power asymmetry, and institutional effectiveness in international relations.

To address concerns of methodological validity and reliability, the study adopts several strategies commonly employed in qualitative research. Source triangulation is used to cross-validate findings across academic literature, legal documents, and policy reports. Reflexivity is maintained throughout the research process to acknowledge the interpretive nature of qualitative analysis and to mitigate potential researcher bias (Creswell & Poth, 2018, pp. 258–263). While the study does not involve primary empirical data or human subjects, ethical considerations related to accurate representation, citation integrity, and analytical transparency are strictly observed.

It is important to clarify that this study does not produce findings through primary data collection or original empirical investigation. Rather, the findings presented in the subsequent section emerge directly from the systematic qualitative literature review, thematic coding, and comparative institutional analysis described above. The four analytical subthemes identified in the findings—normative fragmentation, institutional insufficiency, capacity asymmetries, and legal ambiguity—represent the dominant patterns and structural tensions distilled from the coded and cross-analyzed body of literature. This approach, sometimes termed analytical synthesis or interpretive synthesis (Booth et al., 2016, pp. 82–87), enables the generation of theoretically grounded insights from existing scholarship rather than new empirical data. Finally, the methodological limitations of the study are explicitly acknowledged. As a qualitative and literature-based analysis, the findings are inherently interpretive and may not capture rapidly evolving operational developments in cyberspace. However, by focusing on structural and normative dimensions rather than technical specifics, the study offers durable insights into the regulatory challenges confronting international security regimes. This methodological approach provides a robust foundation for subsequent empirical research and policy-oriented investigations into cyber governance. Table 1 provides an overview of the qualitative research design, data sources, and analytical frameworks guiding this study.

Table 1. Overview of Research Design and Analytical Strategy

Component	Description
Research Design	Qualitative, interpretive analysis
Data Sources	Peer-reviewed academic literature, international legal documents, policy reports
Analytical Methods	Systematic literature review; thematic coding; comparative institutional analysis
Theoretical Frameworks	Realism, regime theory, constructivism
Unit of Analysis	International cyber governance arrangements and security regimes
Scope	Global (state and non-state actors in cyberspace)

III. FINDINGS

The findings presented below are directly derived from the systematic coding and analytical synthesis of the reviewed literature, rather than from primary empirical observation. The qualitative analysis reveals that regulatory challenges in cyber governance are not isolated technical deficiencies but structural features of the contemporary international security environment. Four interrelated analytical subthemes emerge from the literature: normative fragmentation, institutional insufficiency, capacity asymmetries, and persistent legal ambiguity. Together, these findings illustrate how cyberspace disrupts conventional security regimes and complicates efforts to sustain global order through existing regulatory mechanisms.

A. Normative Fragmentation and the Absence of Binding Obligations

One of the most salient findings concerns the fragmented nature of normative frameworks governing state behavior in cyberspace. Despite broad acknowledgment that international law applies to cyberspace, there is no consensus on how existing norms should be interpreted or enforced in practice. Most international agreements related to cyber security rely on voluntary commitments, political declarations, or confidence-building measures rather than legally binding obligations (Nye, 2017, pp. 54–57). This reliance on soft law reflects both political reluctance among major powers and uncertainty regarding attribution and enforcement mechanisms.

Normative fragmentation is further reinforced by divergent strategic cultures and ideological preferences among states. While some actors promote an open, global, and multi-stakeholder vision of cyberspace, others prioritize digital sovereignty and state control over information flows (Tikk & Kerttunen, 2020, pp. 112–118). These competing normative orientations inhibit the consolidation of shared expectations of responsible behavior, increasing the likelihood of misperception and escalation in the cyber domain. As a result, cyber governance lacks the normative clarity typically associated with effective international security regimes.

B. Institutional Insufficiency and Regime Complexity

A second major finding relates to the institutional architecture of cyber governance, which is characterized by regime complexity rather than institutional coherence. Multiple international organizations, regional bodies, and informal forums address cyber-related issues, yet none possess comprehensive regulatory authority or enforcement capacity. United Nations–led processes such as the Group of Governmental Experts and the Open-Ended Working Group have facilitated dialogue but remain constrained by consensus-based decision-making and geopolitical rivalries (United Nations, 2021, pp. 10–15).

This institutional fragmentation produces coordination gaps and overlapping mandates that weaken collective responses to cyber threats. Scholars note that regime complexity can, under certain conditions, enhance flexibility; however, in the security realm, it often undermines predictability and strategic stability (Kello, 2017, pp. 97–102). The findings suggest that cyber governance institutions struggle to translate normative discussions into operational mechanisms

capable of preventing conflict or ensuring accountability, thereby limiting their effectiveness as components of international security regimes.

C. Capacity Asymmetries and Unequal Participation

A third critical finding highlights the role of cyber capacity asymmetries in shaping governance outcomes. States with advanced technological infrastructure and regulatory expertise exert disproportionate influence over agenda-setting and norm development processes. In contrast, many developing states face constraints related to technical skills, financial resources, and institutional capacity, reducing their ability to engage meaningfully in cyber governance forums (Madeline & Mueller, 2021, pp. 656–660).

These disparities contribute to a governance environment in which global cyber norms reflect the interests of a limited group of technologically advanced actors. The case of China illustrates how emerging powers seek to reshape these norms to reflect their own conceptions of digital sovereignty and state control, further complicating prospects for universal regulatory standards (Inkster, 2016, pp. 45–51). Capacity gaps also undermine collective security by creating uneven resilience across the international system, making less-prepared states more vulnerable to cybercrime, espionage, and infrastructure disruption (Betz & Stevens, 2013, pp. 121–126; Liaropoulos, 2017, pp. 3–8). The findings indicate that without systematic capacity-building initiatives, cyber governance risks reinforcing existing global inequalities rather than mitigating shared security threats.

D. Legal Ambiguity and Strategic Exploitation

The final analytical subtheme concerns the persistent legal ambiguity surrounding cyber operations. While international legal principles such as sovereignty, non-intervention, and due diligence are widely referenced, their application to cyber activities remains contested. This ambiguity is particularly pronounced with respect to thresholds for the use of force and the right of self-defense, enabling states to operate in legal gray zones below the threshold of armed conflict (Schmitt, 2017, pp. 30–35).

Landmark cases such as the Stuxnet operation against Iranian nuclear facilities demonstrated how states can conduct sophisticated offensive cyber operations in legal gray zones, exploiting ambiguities around attribution and proportionality (Farwell & Rohozinski, 2011, pp. 25–30). The findings suggest that legal uncertainty incentivizes strategic exploitation, as states may engage in cyber operations while avoiding clear violations of international law. This dynamic weakens deterrence and complicates crisis management, increasing the risk of escalation through miscalculation or misattribution (Mueller, 2020, pp. 84–89). In the absence of clearer legal standards, international security regimes remain ill-equipped to address the full spectrum of cyber threats in a consistent and predictable manner.

Taken together, these findings demonstrate that regulatory challenges in cyber governance are deeply embedded in the structural and normative foundations of the international system. Normative fragmentation, institutional insufficiency, capacity asymmetries, and legal ambiguity interact to produce a governance

environment that struggles to support stable global order. Rather than constituting a temporary transitional phase, these challenges appear to be enduring features of cyber governance, necessitating more comprehensive and adaptive regulatory strategies within international security regimes.

The four analytical subthemes identified in the findings—normative fragmentation, institutional insufficiency, capacity asymmetries, and legal ambiguity—are systematically synthesized in Table 2, which illustrates how these challenges intersect with theoretical debates on sovereignty, regimes, and global order.

Table 2. Regulatory Challenges in Cyber Governance and Their Implications for International Security Regimes

Analytical Dimension	Core Regulatory Challenge	Implications for International Security Regimes	Theoretical Relevance
Normative Frameworks	Fragmentation of norms and reliance on non-binding commitments	Weak predictability and limited accountability among states	Challenges constructivist expectations of norm internalization; highlights power asymmetries in norm diffusion
Institutional Architecture	Regime complexity and lack of centralized authority	Coordination failures and reduced crisis management capacity	Exposes limitations of classical regime theory under technological acceleration
Sovereignty	Tension between territorial sovereignty and non-territorial cyberspace	Erosion of traditional sovereignty-based governance models	Supports relational and socially constructed conceptions of sovereignty
Capacity Distribution	Uneven cyber capabilities between developed and developing states	Marginalization of less-capable states and reduced collective security	Reinforces critical and constructivist critiques of unequal global order
Legal Regulation	Ambiguity in the application of international law to cyber operations	Expansion of strategic “gray zones” and escalation risks	Undermines deterrence logic central to realist security frameworks

Source: Author’s synthesis based on the study’s qualitative analysis and reviewed literature (e.g., Kello, 2017; Nye, 2017; Mueller, 2020; Tikk & Kerttunen, 2020).

IV. DISCUSSION

The findings of this study underscore that cyber governance challenges are not only technical or transitional but also structurally embedded within the contemporary international system. When interpreted through the lens of international relations theory, these challenges illuminate deeper tensions between sovereignty, power, and cooperation in a digitalized global order. Cyber governance thus emerges as a critical site where traditional security paradigms are increasingly strained, necessitating both theoretical refinement and institutional innovation.

A. Cyber Governance and the Limits of Sovereignty

From a realist perspective, the persistence of normative fragmentation and legal ambiguity reflects enduring concerns over sovereignty and relative gains. States remain reluctant to commit to binding cyber regulations due to fears of strategic vulnerability and asymmetric exposure, particularly given the difficulty of attribution in cyberspace (Nye, 2017, pp. 58–61). The findings suggest that cyber governance amplifies classical realist dilemmas, as states prioritize autonomy and deterrence over cooperation, even when facing shared vulnerabilities. This dynamic

reinforces the use of cyberspace as a domain for competitive state behavior below the threshold of armed conflict.

At the same time, the non-territorial nature of cyberspace challenges the very foundations of sovereign control. Unlike conventional domains, cyberspace cannot be fully governed through territorial jurisdiction, rendering unilateral regulatory approaches insufficient (Kello, 2017, pp. 112–117). The findings indicate that this mismatch between sovereign authority and technological reality produces governance gaps that are exploited strategically, thereby destabilizing international security regimes. As such, sovereignty in cyberspace appears increasingly relational rather than absolute, dependent on cooperation, interdependence, and shared norms.

B. Regime Theory and Institutional Fragmentation

Institutional insufficiency and regime complexity identified in the findings align closely with insights from international regime theory. Regimes traditionally function by reducing uncertainty and facilitating cooperation through shared norms and rules (Keohane, 1984, pp. 88–92). However, the cyber domain illustrates the limitations of regime theory when confronted with rapid technological change and geopolitical rivalry. The proliferation of overlapping forums and initiatives reflects not institutional abundance, but institutional weakness, as no single body possesses the authority or legitimacy to coordinate global cyber governance effectively.

The discussion reveals that regime complexity in cyberspace undermines predictability, a core requirement for effective security governance. While some degree of institutional pluralism may foster innovation, excessive fragmentation hinders crisis management and norm internalization (Karns et al., 2015, pp. 211–216). Consequently, cyber governance regimes struggle to perform core security functions such as deterrence stabilization, escalation control, and accountability. This raises important questions about whether existing institutional models are adequate for governing emerging security domains.

C. Power Asymmetry, Inequality, and Normative Authority

The findings related to cyber capacity asymmetries highlight how power disparities shape governance outcomes and normative authority. Constructivist scholarship emphasizes that norms are not neutral but reflect the interests and identities of dominant actors (Finnemore & Sikkink, 1998, pp. 891–895). In cyber governance, technologically advanced states exert disproportionate influence over agenda-setting and norm articulation, often framing their preferences as universal standards.

This asymmetry has significant implications for global order. The marginalization of developing states undermines the legitimacy of emerging cyber norms and weakens collective security by creating uneven resilience across regions (Madeline & Mueller, 2021, pp. 660–664). The discussion suggests that without deliberate capacity-building and inclusive participation mechanisms, cyber governance risks entrenching digital hierarchies that mirror—and potentially exacerbate—existing global inequalities. Such outcomes challenge liberal claims that cyberspace inherently promotes openness and democratization.

D. Legal Ambiguity and Strategic Stability

Legal ambiguity, as identified in the findings, has profound implications for strategic stability in international security regimes. The absence of clear legal thresholds enables states to engage in persistent cyber operations while avoiding overt violations of international law (Schmitt, 2017, pp. 36–40). This practice of operating in the “gray zone” erodes the deterrent value of legal norms and increases the likelihood of miscalculation or unintended escalation (Mueller, 2020, pp. 90–95).

Importantly, scholars such as Rid (2013, pp. 163–168) and Valeriano and Maness (2015, pp. 185–192) offer a corrective to more alarmist readings, demonstrating empirically that most cyber interactions between states remain below the threshold of armed conflict and are subject to tacit restraint. Nevertheless, this restraint is fragile and dependent on shared understandings that lack formal legal codification. From a security governance perspective, this ambiguity weakens crisis management mechanisms by obscuring intent and responsibility. Unlike kinetic conflicts, cyber incidents often unfold incrementally and covertly, complicating diplomatic signaling and response calibration (Betz & Stevens, 2013, pp. 131–136). The discussion therefore suggests that enhancing legal clarity—while challenging—is essential for stabilizing expectations and reinforcing the credibility of international security regimes in cyberspace.

E. Toward Adaptive and Multilayered Governance

Taken together, the findings and their theoretical implications point toward the necessity of adaptive, multilayered governance frameworks. Rather than pursuing comprehensive treaties that are politically infeasible, the discussion supports incremental approaches that combine norm consolidation, institutional coordination, and capacity development (Kello, 2017, pp. 190–196). Public–private partnerships, regional confidence-building measures, and issue-specific agreements may offer pragmatic pathways for reducing fragmentation while respecting sovereignty concerns.

Importantly, cyber governance must be embedded within broader debates on global order rather than treated as a standalone technical issue. As cyberspace increasingly shapes economic, political, and military interactions, its governance becomes inseparable from the future of international security regimes. The discussion thus reinforces the argument that cyber governance represents not a peripheral challenge, but a defining test for the adaptability and relevance of contemporary international order. The theoretical insights and governance implications derived from the discussion are synthesized in Table 3, highlighting how cyber governance challenges reshape international security regimes.

Table 3. Theoretical Insights and Governance Implications of Cyber Governance

Analytical Insight	Theoretical Implication	Implication for International Security Governance
Normative fragmentation	Limits constructivist expectations of norm internalization	Necessitates incremental norm consolidation mechanisms
Institutional complexity	Reveals limits of classical regime theory	Calls for improved coordination among overlapping institutions

Analytical Insight	Theoretical Implication	Implication for International Security Governance
Sovereignty erosion	Supports relational conceptions of sovereignty	Requires cooperative and multilevel governance approaches
Capacity asymmetries	Highlights power-based norm diffusion	Emphasizes inclusive capacity-building strategies
Legal ambiguity	Undermines deterrence and stability	Demands clarification of legal thresholds in cyberspace

Source: Author's synthesis based on discussion and theoretical analysis.

V. CYBER GOVERNANCE AND INTERNATIONAL ORDER: THEORETICAL IMPLICATIONS

The regulatory challenges identified in this study carry significant theoretical implications for how international relations scholarship conceptualizes global order, security regimes, and governance beyond the state. Cyber governance exposes foundational assumptions embedded in dominant IR theories—particularly regarding sovereignty, authority, and institutional effectiveness—and compels a reconsideration of how order is produced and maintained in non-territorial domains. Rather than representing an anomaly, cyberspace increasingly functions as a constitutive arena through which contemporary international order is negotiated and contested (Kello, 2017, pp. 214–219).

Figure 1 visualizes the theoretical argument advanced in this study by demonstrating how cyber governance reshapes sovereignty, institutional authority, and norm formation within international security regimes.

Figure 1. Cyber Governance Framework in International Security Regimes.



This figure illustrates a multilevel cyber governance framework highlighting the interactions among state actors, international norms, multilateral institutions, private sector and civil society actors, enforcement mechanisms, and oversight processes within international security regimes. Adapted from Yusif and Hafeez-Baig (2021).

A. Revisiting Sovereignty in a Non-Territorial Domain

From a theoretical standpoint, cyber governance challenges the traditional Westphalian conception of sovereignty as territorially bounded and hierarchically exercised. While realist approaches continue to emphasize state authority and strategic competition, the findings suggest that sovereignty in cyberspace operates

as a relational and networked practice rather than an absolute condition (Mueller, 2020, pp. 101–106). States retain formal authority, yet their capacity to control digital space depends heavily on transnational infrastructure, private actors, and international cooperation. This decoupling of authority from territory complicates realist expectations regarding control and deterrence, indicating that sovereignty in cyberspace is increasingly negotiated rather than imposed.

Theoretically, this implies a shift from sovereignty as exclusion to sovereignty as coordination. Cyber governance thus reinforces arguments within critical and constructivist traditions that view sovereignty as socially constructed and contingent upon shared norms and practices rather than fixed legal boundaries (Finnemore & Sikkink, 1998, pp. 900–904). The cyber domain highlights how sovereignty can persist symbolically even as its operational content is transformed by technological interdependence.

B. Regime Theory under Conditions of Technological Acceleration

The findings also have important implications for international regime theory. Classical regime theory assumes that cooperation emerges through stable norms, rules, and decision-making procedures that reduce uncertainty and transaction costs (Keohane, 1984, pp. 93–97). Cyber governance, however, reveals the limits of this assumption in contexts characterized by rapid technological change, attribution uncertainty, and asymmetric capabilities. The prevalence of regime complexity in cyberspace suggests that traditional regime models may be insufficient for explaining governance outcomes in emerging security domains.

Rather than converging toward institutional coherence, cyber governance regimes remain fragmented and informal. This challenges the expectation that institutional density necessarily enhances cooperation (Karns et al., 2015, pp. 224–228). Theoretically, cyberspace may represent a case in which regime proliferation substitutes for regime effectiveness, calling for refinements to regime theory that better account for technological volatility and strategic ambiguity.

A. Norms, Power, and Legitimacy in Cyber Governance

Constructivist approaches offer valuable insights into the normative dimensions of cyber governance, particularly regarding how power shapes norm emergence and legitimacy. The findings demonstrate that cyber norms are not neutral technical standards but politically contested constructs shaped by the interests and identities of dominant actors (Tikk & Kerttunen, 2020, pp. 119–124). Technologically advanced states exercise disproportionate normative authority, framing their preferences as universal principles of responsible behavior.

This dynamic reinforces constructivist claims that norm diffusion is inseparable from power relations (Finnemore & Sikkink, 1998, pp. 895–899). In the cyber domain, normative legitimacy is further undermined by capacity asymmetries that limit meaningful participation by developing states. Theoretically, this suggests that cyber governance norms risk weak internalization and shallow compliance unless accompanied by inclusive capacity-building mechanisms that enhance their perceived fairness and universality.

B. Cyber Governance and the Transformation of Global Order

More broadly, cyber governance challenges linear conceptions of global order premised on clearly defined domains and hierarchical authority structures. The findings support the view that contemporary international order is increasingly characterized by hybridity, where formal institutions coexist with informal norms, public–private governance arrangements, and decentralized authority (DeNardis, 2014, pp. 152–157). Cyberspace accelerates this transformation by amplifying the role of non-state actors and technical communities in security governance.

Theoretically, this implies that global order should be conceptualized less as a fixed structure and more as an evolving process shaped by technological change and normative contestation. Cyber governance thus serves as a critical testing ground for IR theory, revealing the need for analytical frameworks capable of integrating security, governance, and technology within a single conceptual lens (Nye, 2017, pp. 63–66).

C. Theoretical Contribution of the Study

By synthesizing insights from realism, regime theory, and constructivism, this article contributes to international relations scholarship in three key ways. First, it demonstrates that cyber governance exposes structural tensions within existing theories of international order rather than fitting neatly within them. Second, it highlights the need to reconceptualize sovereignty, regimes, and norms in light of non-territorial security challenges. Third, it positions cyber governance as a central—rather than peripheral—component of contemporary international security regimes. In doing so, the study advances the argument that cyberspace is not simply another domain to be governed, but a transformative arena that reshapes the theoretical foundations of global order itself.

CONCLUSION

This study has examined cyber governance as a critical regulatory challenge confronting contemporary international security regimes and the broader structure of global order. By integrating insights from international relations theory, international law, and cybersecurity studies, the article demonstrates that cyberspace is not merely an additional technical domain, but a transformative arena that exposes foundational limitations within existing governance frameworks. The findings reveal that normative fragmentation, institutional insufficiency, capacity asymmetries, and legal ambiguity are not temporary deficiencies, but structural characteristics of cyber governance embedded in the evolving international system.

The analysis shows that traditional security regimes—designed around territorial sovereignty, identifiable actors, and enforceable legal norms—are increasingly ill-equipped to regulate a domain defined by transnational infrastructure, distributed agency, and rapid technological change. As a result, cyber governance has developed through informal norms, fragmented institutions, and voluntary commitments rather than binding regulatory mechanisms. While these arrangements have enabled dialogue and limited cooperation, they fall short of providing the predictability, accountability, and inclusiveness necessary for sustaining international security in the digital age.

By situating these challenges within core international relations theories, the article advances several theoretical contributions. First, it demonstrates that cyber governance fundamentally challenges Westphalian conceptions of sovereignty by decoupling authority from territory and emphasizing relational, network-based forms of control. Second, it reveals the limits of classical regime theory under conditions of technological acceleration and strategic ambiguity, where regime proliferation does not necessarily translate into regime effectiveness. Third, it underscores how power asymmetries shape norm formation and legitimacy in cyberspace, reinforcing constructivist claims that norms are socially constructed and unevenly internalized across the international system.

From a policy perspective, the study highlights the need for adaptive and multilayered governance approaches that move beyond the pursuit of comprehensive treaties. Incremental norm consolidation, enhanced institutional coordination, public–private partnerships, and sustained cyber capacity-building initiatives—particularly for developing states—emerge as essential components of a more resilient governance architecture. Importantly, such efforts must be embedded within broader debates on global order rather than treated as isolated technical solutions.

In direct response to the research questions posed in the introduction, this study arrives at the following conclusions. First, the principal regulatory challenges confronting cyber governance within international security regimes are normative fragmentation, institutional insufficiency, persistent capacity asymmetries between technologically advanced and developing states, and legal ambiguity surrounding the application of international law to cyber operations. These challenges are not peripheral or temporary; they are structurally embedded in the contemporary international system and mutually reinforcing. Second, existing theoretical frameworks in international relations—while offering partial explanatory value—each reach their limits when confronted with cyberspace. Realism explains state reluctance to commit to binding norms and the logic of competitive advantage, but cannot fully account for the governance deficits produced by non-territorial domains and distributed agency. Regime theory illuminates why cooperation remains possible but also reveals how institutional proliferation can substitute for institutional effectiveness. Constructivism offers the most useful lens for understanding normative contestation and the politics of norm diffusion, but must be supplemented by attention to power asymmetries that constrain meaningful participation by weaker states. Third, the most appropriate governance approaches for cyberspace are adaptive and multilayered: incremental norm consolidation through diplomatic processes, enhanced coordination among existing international institutions, public–private partnership frameworks with clearly defined accountability mechanisms, and sustained capacity-building initiatives aimed at reducing the cyber capability gap between developed and developing states. Ultimately, this article argues that cyber governance constitutes a defining test for the adaptability and relevance of international security regimes in the 21st century. As digital technologies continue to reshape political, economic, and military

interactions, the capacity of the international community to regulate cyberspace will play a decisive role in determining whether global order evolves toward greater stability or deeper fragmentation. Future research should build on this framework by examining regional governance models, norm internalization processes, and the long term implications of emerging technologies—including artificial intelligence and quantum computing—for cyber governance and international order transformation (Choucri, 2012, pp. 215–221; Cavelty, 2014, pp. 709–713). In this respect, cyber governance should be understood not as a peripheral policy domain, but as a foundational arena reshaping the future of international order itself.

Statement of Research and Publication Ethics

This article has been prepared in full accordance with the research and publication ethics principles of Yönetim ve Ekonomi Dergisi at all stages of the research and writing process.

Author Contribution Statement

This article is single-authored. The author is solely responsible for all aspects of the work, including conceptualization, literature review, analysis, and writing.

Conflict of Interest Statement

The author declares that there are no conflicts of interest with any individual or organization with respect to this article.

REFERENCES

- Betz, D. J., & Stevens, T. (2013). *Cyberspace and the state: Toward a strategy for cyber-power*. Routledge.
- Booth, W. C., Colomb, G. G., & Williams, J. M. (2016). *The craft of research* (4th ed.). University of Chicago Press.
- Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). Sage.
- Deibert, R. (2019). *Reset: Reclaiming the Internet for civil society*. House of Anansi Press.
- DeNardis, L. (2014). *The global war for Internet governance*. Yale University Press.
- Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. *International Organization*, 52(4), 887–917. <https://doi.org/10.1162/002081898550789>
- Karns, M. P., Mingst, K. A., & Stiles, K. M. (2015). *International organizations: The politics and processes of global governance* (3rd ed.). Lynne Rienner.
- Keohane, R. O. (1984). *After hegemony: Cooperation and discord in the world political economy*. Princeton University Press.
- Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.
- Madeline, C., & Mueller, M. (2021). Cyber capacity building and the uneven distribution of power in global cyber governance. *International Studies Review*, 23(3), 647–670. <https://doi.org/10.1093/isr/viaa089>
- Mueller, M. (2020). *Networks and states: The global politics of Internet governance*. MIT Press.
- Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security*, 41(3), 44–71. https://doi.org/10.1162/ISEC_a_00266
- Saldaña, J. (2016). *The coding manual for qualitative researchers* (3rd ed.). Sage.
- Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.
- Tikk, E., & Kerttunen, M. (2020). *International cyber norms: Legal, policy and industry perspectives*. Oxford University Press.

- United Nations. (2021). *Report of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security*. United Nations General Assembly.
- Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. *Journal of Applied Security Research*, 16(4), 1–24. <https://doi.org/10.1080/19361610.2021.1918995>
- Cavelty, M. D. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics*, 20(3), 701–715. <https://doi.org/10.1007/s11948-014-9549-3>
- Choucri, N. (2012). *Cyberpolitics in international relations*. MIT Press.
- Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, 92(1), 43–62. <https://doi.org/10.1111/1468-2346.12504>
- Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, 53(1), 23–40. <https://doi.org/10.1080/00396338.2011.555586>
- Guitton, C. (2013). Cyber insecurity as a national threat: Overreaction from Germany, France and the UK? *European Security*, 22(1), 21–35. <https://doi.org/10.1080/09662839.2012.749864>
- Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, 53(4), 1155–1175. <https://doi.org/10.1111/j.1468-2478.2009.00572.x>
- Healey, J. (Ed.). (2013). *A fierce domain: Conflict in cyberspace, 1986 to 2012*. Atlantic Council.
- Inkster, N. (2016). *China's cyber power*. International Institute for Strategic Studies / Routledge.
- Klimburg, A. (2017). *The darkening web: The war for cyberspace*. Penguin Press.
- Liaropoulos, A. (2017). Reconceptualising cyber security: Safeguarding human rights and civilian infrastructure in cyberspace. *Journal of Information Warfare*, 16(1), 1–14.
- Rid, T. (2013). *Cyber war will not take place*. Oxford University Press.
- Roff, H. M. (2016). Cyber stability, cyber uncertainty, and the International Committee of the Red Cross. *Ethics and Information Technology*, 18(3), 159–169. <https://doi.org/10.1007/s10676-016-9403-1>
- Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press.