Cybersecurity Obligations for Critical Infrastructure: Emerging Legal Norms, Enforcement Gaps, and Governance Challenges

1. Devika Sharma: Department of Law, University of Delhi, Delhi, India
2. Sandeep Reddy*: Department of Private Law, NALSAR University of Law, Hyderabad, India
3. Hamza Shahid: Department of Law, University of the Punjab, Lahore, Pakistan
***Correspondence: e-mail: sandeep.reddy@nalsar.ac.in**

Abstract

Critical infrastructure has become a focal point of global cybersecurity governance as escalating cyber threats increasingly target essential services such as energy, water, transportation, healthcare, and financial systems. This article examines the evolving legal landscape that governs cybersecurity obligations for critical infrastructure, tracing the transition from voluntary, principles-based frameworks toward binding statutory requirements that impose enforceable duties on operators. Through a narrative review and descriptive analysis of national regulations, international norms, sector-specific obligations, and emerging technological considerations, the study maps the diverse instruments shaping current governance models. The analysis highlights significant advancements, including strengthened incident reporting mandates, growing supply chain accountability, and the incorporation of cybersecurity into broader national security strategies. At the same time, the article identifies persistent enforcement gaps and structural weaknesses that undermine regulatory effectiveness. These challenges include fragmented legal approaches, capacity limitations within industry, jurisdictional conflicts in cross-border cyber operations, difficulties in attributing attacks, ambiguous public-private role divisions, insufficient supply chain oversight, and the paradoxical effects of national security secrecy on transparency and accountability. The article argues that while emerging legal norms represent substantial progress, they remain insufficient without coherent enforcement mechanisms, institutional coordination, and supportive operational capacities. Strengthening critical infrastructure cybersecurity will require integrated regulatory architectures, harmonized international cooperation, enhanced public-private collaboration, and adaptive governance capable of responding to rapidly evolving technologies and threat dynamics. The findings offer a foundational understanding of the current state of legal obligations and illuminate the systemic issues that must be addressed to ensure resilient and effective protection of critical infrastructure worldwide.

Keywords: Critical infrastructure, cybersecurity law, enforcement gaps, regulatory governance, supply chain security, national security, cyber resilience, international norms

Received: date: 12 May 2023
Revised: date: 14 June 2023
Accepted: date: 29 June 2023
Published: date: 01 July 2023

Citation: Sharma, D., Reddy, S., & Shahid, H. (2023). Cybersecurity Obligations for Critical Infrastructure: Emerging Legal Norms, Enforcement Gaps, and Governance Challenges. *Legal Studies in Digital Age*, 2(3), 49-63.

1. Introduction

The concept of critical infrastructure has become central to contemporary cybersecurity governance because it encompasses the physical and digital systems whose disruption would endanger national security, public welfare, and economic stability. These systems include energy grids, water treatment facilities, transportation networks, healthcare institutions, telecommunications backbones, and financial market infrastructures, all of which depend on continuous and reliable operation.

The legal and political significance of critical infrastructure cybersecurity emerges from the fact that these systems constitute the backbone of state functionality; when they are compromised, cascading failures can unfold across borders and sectors, amplifying the magnitude of harm. Scholars examining national protection frameworks increasingly emphasize that safeguarding critical infrastructure requires coordinated policies that reflect the political stakes involved, as disruptions create both domestic vulnerabilities and geopolitical leverage points, particularly as states increasingly integrate cyber operations into broader strategic behavior. These dynamics underscore the importance of treating infrastructure protection not merely as a technical domain but as a legal and institutional priority, a perspective reinforced through research highlighting how states develop cybersecurity policies to protect essential services while adapting administrative structures to match emerging threats (Adegbite et al., 2023). Additionally, the importance of legally framed protective mechanisms is reflected in studies examining how investments in infrastructure must be supported through institutional designs that promote resilience and ensure compliance with state obligations, since the absence of such designs leaves vital systems exposed to strategic exploitation (Zatonatskiy & Lavrentiev, 2023).

The escalation of cyberattacks targeting critical infrastructure illustrates the alarming evolution of the threat landscape. Numerous analyses reveal that state-sponsored actors, criminal syndicates, and opportunistic hackers increasingly focus on disrupting essential services because these targets maximize political, social, and economic impact. Comparative legal scholarship shows that ransomware campaigns, coordinated espionage operations, and destructive malware increasingly penetrate critical systems, exploiting both technological weaknesses and regulatory gaps (Takuro, 2023). Global incidents have demonstrated the vulnerability of energy pipelines, electric grids, hospital networks, and transportation control systems, with research documenting how the sophistication of these attacks continues to deepen in both scale and strategic intention (Tiwari, 2022). Emerging legal and policy discussions emphasize that attacks on healthcare systems, for instance, not only threaten service availability but also heighten privacy risks, creating multidimensional harm that challenges existing oversight mechanisms (Irawati, 2023). Scholars examining public administration highlight that cyber risks to infrastructure increasingly merge with risks to data integrity, confidentiality, and state-level operational continuity, making the stakes of these attacks broader than ever before (Zhyvylo & Shevchenko, 2022). Even regional analyses of cybersecurity governance observe that national and supranational bodies struggle to keep pace with the shifting techniques employed by attackers, whose operations frequently exploit cross-border legal ambiguities and jurisdictional fragmentation (Orji, 2022). As a result, global escalation in threats is not only technical but deeply institutional, revealing weaknesses in legal coordination frameworks meant to govern the protection of critical systems.

Digital transformation has dramatically expanded the vulnerability surface of critical infrastructure by merging information technology networks with operational control systems in ways that introduce unprecedented complexity. The convergence of IT and operational technology has created interdependent ecosystems that enable efficiency and automation but also expose once-isolated industrial control systems to cyber intrusions. Studies examining cybersecurity maturity in public institutions underscore how digital innovation, while beneficial, introduces risk when systems are modernized without corresponding investment in layered security governance (Hochstetter et al., 2023). Infrastructure reliant on IoT devices and cloud-based communication platforms amplifies risk because these components frequently lack robust security-by-design standards and are managed by diverse vendors across global supply chains. Research assessing cybercrime policy frameworks notes that the expansion of interconnected devices provides attackers with multiple entry points, enabling lateral movement through networks that once operated independently (Savchuk, 2023). The adoption of SCADA systems for real-time monitoring and automated control has similarly been highlighted as a structural vulnerability, as these systems rely on protocols that were not originally built with cybersecurity considerations in mind. Analyses of digital financial market infrastructure illustrate how modernization efforts, such as the introduction of digital currency systems, introduce regulatory challenges by expanding the attack surface across both cyber and operational domains (Bakhtiyar et al., 2023). The integration of artificial intelligence and machine learning technologies into infrastructure management also raises new concerns, as regulatory scholars have shown that AI-enabled systems can increase operational efficiency while simultaneously creating opaque vulnerabilities that are difficult for traditional oversight models to address (Oluoha et al., 2022). These developments collectively demonstrate that technological

transformation, while essential for modernization, simultaneously magnifies risk by broadening the space in which legal frameworks must operate to ensure adequate protection.

The legal problem underpinning critical infrastructure cybersecurity arises from fragmented, outdated, or voluntary frameworks that fail to respond adequately to contemporary threat realities. Comparative legal studies show that while several jurisdictions have adopted national cybersecurity strategies, many still rely heavily on voluntary standards and non-binding guidelines that lack strong enforcement mechanisms (Kashyap & Chaudhary, 2023). Scholars examining institutional cybersecurity models argue that the absence of unified statutory obligations leads to significant inconsistencies across sectors, with some industries possessing detailed mandates while others operate with minimal regulatory oversight (Savchuk, 2023). Analyses of Canadian and European legal approaches demonstrate that even when governments introduce comprehensive legislation, such frameworks often remain misaligned with technological developments, creating compliance gaps that adversaries can exploit (Malone & Walton, 2023). The challenges extend to infrastructure investment governance, where research indicates that inadequate institutional support and absence of clear regulatory standards undermine the durability and security of critical systems (Zatonatskiy & Lavrentiev, 2023). Scholars exploring national security law further highlight that administrative bodies responsible for cybersecurity governance frequently lack the legal authority or resources necessary to enforce compliance, creating vulnerabilities that stem more from institutional design weaknesses than from technological shortcomings (Макарчук, 2021). Research on coordinated threat intelligence frameworks reinforces this problem by showing that fragmented legal arrangements hinder real-time information sharing between public and private actors, thereby weakening the overall responsiveness of national cybersecurity ecosystems (Ndubuisi, 2023). These findings indicate that current legal frameworks struggle to keep pace with adversarial innovation, resulting in a governance architecture that remains inadequate for addressing rapidly evolving cyber threats.

This narrative review employs a descriptive analysis method that synthesizes insights from laws, regulatory frameworks, policy documents, international standards, and interdisciplinary scholarly literature to illuminate these tensions. The approach enables examination of how different jurisdictions conceptualize critical infrastructure protection within their legal systems and how institutional, administrative, and technical factors interact to shape regulatory effectiveness. Research emphasizing institutional and administrative design in cybersecurity governance provides key analytical grounding for understanding how legal mandates translate into operational practices across sectors (Savchuk, 2023). Studies addressing real-time collaboration mechanisms inform the analysis of enforcement gaps by demonstrating the essential role of coordinated communication networks in supporting legal compliance (Ndubuisi, 2023). Scholarship on the legitimacy of cybersecurity frameworks contributes conceptual tools for interpreting how states justify protective measures amid growing securitization of digital environments (Thumfart, 2022). Work examining global cyber conflict and nation-state operations provides deeper contextualization for the legal and political salience of infrastructure protection, illustrating why governance models must adapt to internationalized threat patterns (Tiwari, 2022). Analyses of third-party risk in infrastructure projects additionally reveal how legal obligations must account for multi-actor ecosystems in which vulnerabilities emerge through complex contractual and operational relationships (Nathaniel et al., 2022). The descriptive analysis thus draws from diverse scholarly and policy domains to assess the adequacy of emerging norms and identify gaps that impede comprehensive protection.

The purpose of this article is to examine emerging legal norms governing critical infrastructure cybersecurity, assess their adequacy in the context of escalating threats and rapid digital transformation, and identify the regulatory and enforcement gaps that continue to undermine effective protection of vital systems.

2. Mapping the Landscape of Cybersecurity Obligations for Critical Infrastructure

The regulatory landscape governing cybersecurity obligations for critical infrastructure reflects a multilayered and evolving system of national, regional, and international instruments that together form a fragmented yet increasingly interconnected governance framework. At the national level, states have developed a variety of regulatory models that impose obligations on operators of essential services to safeguard infrastructure from cyber threats. In the United States, the NIST Cybersecurity Framework represents one of the most influential voluntary models, emphasizing risk assessment, continuous monitoring, incident response planning, and resilience-based governance. Although voluntary in nature, the framework has been widely

adopted across public and private sectors, illustrating how soft-law instruments can shape national cybersecurity behavior even in the absence of statutory force. A comparable yet more mandatory approach is reflected in the European Union's NIS2 Directive, which expands sectoral coverage, strengthens incident reporting requirements, and introduces significant penalties for non-compliance. Analyses of comparative regulatory development demonstrate how mandatory frameworks such as NIS2 reflect a shift toward stronger legal obligations as cyber threats intensify, with similar trends observable in Canadian and European legislative debates that explore the scope of duties for operators of critical cyber systems (Malone & Walton, 2023). Other jurisdictions, including Singapore and Australia, enforce stricter statutory schemes through instruments such as the Singapore Cybersecurity Act and Australia's Security of Critical Infrastructure Act, each of which establishes licensing regimes, reporting obligations, and government intervention powers. Research examining national strategies for infrastructure protection highlights that these regulatory regimes increasingly emphasize national security imperatives, linking infrastructure governance to broader administrative capacities for implementing state cybersecurity policy (Adegbite et al., 2023). Such national frameworks underscore the diversity of regulatory approaches globally, revealing differences in sectoral scope, enforcement powers, and the balance between voluntary guidance and binding obligations.

Beyond national systems, international norms and soft-law frameworks provide additional layers of cybersecurity governance relevant to critical infrastructure. The Budapest Convention remains the primary international treaty addressing cybercrime, establishing mechanisms for cooperation, procedural safeguards, and harmonization of national criminal laws. Although not specifically targeted at critical infrastructure, its provisions on unauthorized access, data interference, and system integrity contribute to a broader protective environment. Research assessing cybercrime legal models emphasizes how such instruments support national legal regimes by offering shared definitions and cooperation channels (Savchuk, 2023). The Tallinn Manual, although non-binding, offers significant insights into how international law applies to cyber operations affecting infrastructure, particularly in interpreting state responsibility, due diligence, and thresholds for use of force. Analyses of state-sponsored cyber activities highlight how norms derived from such manuals help guide assessments of legality when infrastructure disruptions result from international conflict or covert operations (Tiwari, 2022). At the level of the United Nations, dialogues within the Group of Governmental Experts and the Open-Ended Working Group reinforce voluntary principles concerning responsible state behavior, such as avoiding attacks on critical infrastructure during peacetime and cooperating to mitigate malicious cyber activity. Regional studies of African cybersecurity policy responses add context on how states interpret these norms in regional frameworks, emphasizing the importance of harmonized legal responses to cross-border cyber threats (Orji, 2022). Beyond institutional norms, technical standards such as the ISO/IEC 27000 series serve as global benchmarks for information security management. Research analyzing information security maturity in public institutions demonstrates how international standards can guide national regulatory compliance by providing practical frameworks for risk management, control implementation, and continuous improvement (Hochstetter et al., 2023). These international instruments, while varied in scope and legal status, collectively contribute to a global normative environment that shapes how states conceptualize cybersecurity obligations for critical infrastructure.

Sector-specific regulatory obligations further diversify the legal landscape, as different industries face unique operational risks and technological configurations. In the energy sector, governments often impose stringent requirements due to the cascading impact of outages on national stability. Mandatory reporting of cyber incidents, protective measures for industrial control systems, and risk assessment obligations reflect a high level of regulatory scrutiny. Water infrastructure faces similar obligations, particularly regarding operational technology protection and continuity of service, with risk-based requirements that emphasize resilience and redundancy. Aviation cybersecurity obligations, grounded in both national law and international civil aviation standards, focus on securing communication systems, air traffic management networks, and digital components integrated into modern aircraft. Health systems, meanwhile, operate under hybrid frameworks that integrate data protection obligations with infrastructure-specific technical safeguards. Studies examining post-pandemic healthcare governance highlight the legal importance of hospitals maintaining cybersecurity mechanisms that protect patient rights and ensure uninterrupted service delivery, illustrating how regulatory duties intersect with broader health law principles (Irawati, 2023). Financial services represent one of the most heavily regulated sectors, with obligations that extend across fraud prevention, payment system protection, digital currency governance, and interbank communication networks. Research analyzing legal frameworks for modernizing financial market infrastructure demonstrates how digital transformations—such as the

introduction of digital currencies—produce new regulatory duties related to system integrity, cryptographic standards, and national financial stability (Bakhtiyar et al., 2023). These sectoral variations reflect the necessity of tailoring cybersecurity obligations to operational contexts while preserving overarching legal principles related to risk mitigation and infrastructure resilience.

The governance models used to shape these obligations range from voluntary guidelines to mandatory compliance regimes, each offering distinct advantages and challenges. Voluntary frameworks, such as the NIST model, rely on flexibility and industry buy-in, enabling rapid adaptation to technological advances without the delays associated with statutory reform. However, research evaluating institutional cybersecurity structures emphasizes that voluntary approaches may leave critical gaps in sectors with lower maturity or limited resources, as inconsistent adoption undermines national resilience (Savchuk, 2023). Mandatory compliance frameworks, such as the EU's NIS2 Directive or Australia's SOCI Act, impose clear obligations backed by enforcement mechanisms, creating stronger incentives for risk management and incident reporting. Comparative analyses show that these frameworks help address systemic vulnerabilities by establishing uniform standards across sectors (Malone & Walton, 2023). Risk-based regulatory models, which adapt obligations to the specific threat exposure of each sector or operator, are increasingly favored because they align legal requirements with practical security needs. Research exploring the governance of third-party risk in infrastructure projects highlights the importance of risk-based obligations in complex ecosystems where vulnerabilities arise not only from primary operators but also from contractors, vendors, and private partners (Nathaniel et al., 2022). Resilience-centered governance, which emphasizes continuity of operations and rapid recovery, complements traditional security measures by recognizing that infrastructure disruptions cannot always be prevented. Studies on cybersecurity maturity in public-sector institutions illustrate how resilience-based models strengthen institutional capacity by ensuring that systems remain functional even when breaches occur (Hochstetter et al., 2023). These governance approaches collectively reveal the spectrum of legal philosophies shaping infrastructure protection, from strict regulatory mandates to adaptive, context-sensitive models.

Despite significant variation across jurisdictions and sectors, several common obligations recur throughout cybersecurity frameworks for critical infrastructure. Incident reporting remains one of the most universal duties, requiring operators to alert authorities or regulatory agencies when cyber incidents occur. Mandatory reporting enables governments to detect systemic threats, support sectoral coordination, and initiate emergency responses, although studies examining coordinated threat intelligence frameworks emphasize that reporting obligations are only effective when supported by real-time collaboration mechanisms (Ndubuisi, 2023). Risk assessment obligations—often mandated by national law or guided by international standards—require operators to identify vulnerabilities, evaluate potential consequences, and implement mitigation strategies. Supply chain security has become a critical area of focus due to the complex global networks that underpin infrastructure operations, with research on digital financial systems demonstrating how third-party vulnerabilities create systemic risk points (Bakhtiyar et al., 2023). Obligations related to operational continuity require operators to maintain backup systems, disaster recovery plans, and redundancy mechanisms to ensure service availability even in cases of severe disruption. Critical event management duties often include coordination with governmental bodies, implementation of emergency communication protocols, and participation in national cyber exercises. Encryption standards and data protection measures represent another category of obligations, particularly in sectors where confidentiality and integrity of data are essential, such as healthcare and public administration. Scholars analyzing cybersecurity and privacy risks in public-sector systems emphasize that effective encryption and access control mechanisms are indispensable for safeguarding sensitive national data (Zhyvylo & Shevchenko, 2022). These common obligations illustrate the foundational elements of cybersecurity governance, forming a baseline that operators must meet regardless of sector or jurisdiction.

Taken together, the national regulatory frameworks, international norms, sector-specific obligations, governance models, and common legal duties reviewed in this section reveal a landscape that is both comprehensive and uneven. While some jurisdictions have adopted robust, mandatory frameworks backed by enforcement powers, others rely heavily on voluntary standards and soft-law instruments that lack consistency and accountability mechanisms. Sectoral variations reflect differing operational risks and regulatory traditions, while international norms provide overarching principles that guide interpretation and coordination but do not impose binding obligations. The resulting picture is one of significant global progress accompanied

by persistent disparities, creating a complex and fragmented regulatory environment in which critical infrastructure operators must navigate diverse expectations and evolving threats. This mapping establishes the descriptive baseline necessary to evaluate emerging norms, assess regulatory adequacy, and identify the enforcement gaps that persist across global cybersecurity governance.

3. Emerging Legal Norms: From Voluntary Standards to Hard Law

Emerging legal norms in the field of critical infrastructure cybersecurity reflect a decisive global shift from voluntary, principles-based guidance toward binding, enforceable regulatory obligations. This transformation is driven by the recognition that soft norms, while influential in shaping organizational behavior, are insufficient to address the escalating scale, sophistication, and geopolitical complexity of contemporary cyber threats. Frameworks such as the **National Institute of Standards and Technology** Cybersecurity Framework, ISO/IEC standards developed by **International Organization for Standardization**, and general OECD digital security principles have long served as foundational reference points, offering risk-management guidance that organizations could adopt voluntarily based on sectoral needs and institutional maturity. However, the increasing legal and political sensitivity of critical infrastructure has prompted many jurisdictions to move from discretionary adoption to statutory imposition. The European Union's NIS2 Directive illustrates this evolution, transforming the earlier flexible compliance model into a regime built on mandatory standards, stringent incident reporting, oversight audits, and substantial administrative penalties. Comparative legal analyses examining developments in Europe and North America demonstrate that regulators are increasingly unwilling to rely solely on soft-law mechanisms, as evidenced by discussions surrounding Canada's proposed Critical Cyber Systems Protection Act that parallel the binding orientation of NIS2 (Malone & Walton, 2023). This global movement signals a normative transition in which voluntary frameworks serve as conceptual precursors to more robust legal mandates that embed risk management and resilience into enforceable statutory obligations.

One of the defining features of emerging cybersecurity law is the growing emphasis on supply chain accountability and third-party risk management. Critical infrastructure systems rely on complex, globally distributed networks of vendors, cloud service providers, hardware manufacturers, and subcontractors, making indirect vulnerabilities a central legal concern. Scholars examining infrastructure project governance show that disruptions arising from external partners can undermine service continuity, thereby expanding the legal responsibility of operators to include oversight of vendors and subcontracted entities (Nathaniel et al., 2022). In the financial sector, modernization efforts such as the integration of digital currencies reveal how vulnerabilities in third-party technological systems can produce systemic risks and thus require regulatory frameworks that hold both operators and their suppliers accountable (Bakhtiyar et al., 2023). International studies of cybersecurity law evolution argue that emerging legal frameworks increasingly mandate "security-by-design" principles, obligating operators and manufacturers to integrate technical safeguards throughout the product lifecycle rather than relying solely on post-deployment interventions (Takuro, 2023). This shift reflects an understanding that resilience cannot be achieved if upstream dependencies remain unregulated. Consequently, statutory obligations now frequently incorporate requirements for continuous monitoring of vendor performance, contractual risk allocation, supply chain transparency, and formal verification of third-party security practices. This expansion of responsibility represents a structural shift in cybersecurity governance, compelling organizations to adopt holistic risk-management approaches grounded in legal accountability for interconnected systems.

Cross-border regulatory cooperation is another essential component of emerging cybersecurity norms, reflecting the transnational nature of critical infrastructure operations and the globalized threat environment. The European Union and the United States have intensified dialogues concerning cybersecurity alignment, particularly in areas such as information sharing, supply chain security, and the protection of digital service providers. QUAD initiatives involving the United States, Japan, India, and Australia similarly illustrate the emergence of international coalitions dedicated to strengthening regional security architectures, including those associated with critical infrastructure protection. Regional agreements within Africa have also been examined as important frameworks for coordinating legal responses to cyber operations, particularly as states confront increasing risks posed by hostile actors targeting essential services (Orji, 2022). Global cooperation efforts within United Nations bodies, including the Group of Governmental Experts and the Open-Ended Working Group, have reinforced the importance of responsible state behavior norms, such as refraining from attacking critical infrastructure during peacetime and

assisting other states in mitigating malicious cyber activity. These initiatives collectively contribute to the formation of an international normative ecosystem in which national laws increasingly reflect shared expectations and cooperative mechanisms. As cyber threats transcend borders, legal frameworks are moving toward harmonization, enabling states to implement consistent regulatory obligations that address the distributed nature of modern infrastructure systems.

At the national level, one of the most significant developments reshaping the legal landscape is the rise of a "duty of care" and a "standard of reasonable cybersecurity" within tort and administrative law. These emerging doctrines hold operators of essential services legally responsible when failures in cybersecurity governance result in foreseeable harm. Scholars examining the institutional structures of state cybersecurity policies argue that administrative bodies increasingly require organizations to demonstrate not merely compliance with technical standards but adherence to broader principles of due diligence and responsible system stewardship (Savchuk, 2023). Courts in several jurisdictions have begun referencing international standards such as ISO/IEC 27001 as indicators of what constitutes reasonable security practice, thereby transforming soft norms into quasi-legal benchmarks. The concept of duty of care also intersects with broader national security considerations, as failures in infrastructure protection can create cascading harm across entire economies. Analyses of administrative law frameworks in the security sector highlight that national security bodies increasingly conceptualize cyber obligations as integral to state defense strategies, embedding them within the legal architecture governing national resilience (Макарчук, 2021). This doctrinal evolution illustrates the trend toward linking cybersecurity not only to information governance but to broader legal principles concerning public safety, state responsibility, and societal risk.

As these legal norms expand in scope, governments worldwide are increasingly framing critical infrastructure cybersecurity as a national security imperative rather than a purely technical or administrative concern. Research analyzing state cybersecurity strategies shows that governments now consider disruptions to essential services as threats comparable to traditional national security risks, requiring coordination across defense, intelligence, law enforcement, and regulatory sectors (Adegbite et al., 2023). This shift is particularly evident in legal frameworks that grant governments emergency powers to intervene in private infrastructure operations, mandate intelligence sharing, or impose enhanced vetting for high-risk vendors. Studies addressing the institutional role of law enforcement bodies in national security policy underscore the growing integration of cybersecurity mandates into administrative and defense structures, reinforcing the idea that cyber governance must be embedded within broader security doctrines rather than isolated technical regulations (Макарчук, 2021). As a result, operators of essential services increasingly face not only administrative compliance requirements but obligations that carry national security implications, linking their responsibilities to state stability and geopolitical resilience.

Technological evolution further influences the emergence of new legal norms, particularly as artificial intelligence, quantum technologies, and advanced simulation tools introduce new risk domains. AI-enabled systems are now widely used in monitoring, predictive maintenance, intrusion detection, and operational decision-making. However, regulatory scholarship highlights how these tools also create opaque vulnerabilities, raising concerns about algorithmic accountability and the potential for AI systems to amplify system-level risks if compromised (Oluoha et al., 2022). As infrastructure operators adopt machine learning tools for autonomous or semi-autonomous functions, legal frameworks increasingly require transparency, auditability, and bias mitigation to ensure that automated processes do not undermine system security. Quantum-resistant cryptography has emerged as another critical domain, as the eventual development of quantum computing capabilities threatens to render existing encryption systems obsolete. Scholars examining cybersecurity law evolution argue that emerging regulations will likely require operators to adopt quantum-safe algorithms as part of forward-looking resilience obligations (Takuro, 2023). Digital twin technologies—virtual replicas of physical infrastructure used for testing and simulation—also raise legal questions about data integrity, model accuracy, and cross-system risks, especially as adversaries may target digital twins to manipulate operational decisions. Studies focused on national infrastructure policy note that regulators are beginning to view such technologies as integral components of risk management frameworks, requiring governance mechanisms that address not only physical infrastructure but its digital representations (Zatonatskiy & Lavrentiev, 2023). These technological developments illustrate how emerging legal norms must adapt dynamically to evolving capabilities, ensuring that cybersecurity obligations remain relevant in environments characterized by continual innovation.

The shift from voluntary standards to binding legal mandates is accelerated by pressures from increasingly severe cyber incidents, rising geopolitical tensions, and growing public awareness of infrastructure vulnerabilities. Scholars examining

global cyber conflict argue that infrastructure has become both a strategic target and a battleground for state competition, compelling governments to adopt stricter protective frameworks as a matter of national defense (Tiwari, 2022). Research focused on coordinated threat intelligence underscores how the scale and speed of contemporary cyberattacks require real-time collaboration between public and private actors, leading to legal obligations that mandate participation in information-sharing networks (Ndubuisi, 2023). Even environmental policy critiques reflect broader concerns about governance failures in complex systems, offering insights into how inadequate regulatory frameworks can undermine societal resilience in domains requiring continuous oversight (S., 2023). The convergence of these pressures has created a normative environment in which states increasingly view cybersecurity obligations as essential tools for managing systemic risk and ensuring long-term national stability.

Taken together, these developments demonstrate a clear trajectory toward more binding, institutionalized, and enforceable legal norms governing critical infrastructure cybersecurity. The movement from voluntary standards to statutory obligations, the expansion of supply chain accountability, the rise of cross-border cooperation, the emergence of negligence-based liability doctrines, the integration of cybersecurity into national security frameworks, and the influence of advanced technologies collectively reshape the regulatory environment. As a result, operators of essential services now face a governance landscape in which compliance is no longer optional but a legally enforceable necessity grounded in evolving global expectations and heightened risk realities.

4. Enforcement Gaps and Regulatory Incoherence: Challenges to Effective Governance

The enforcement landscape surrounding critical infrastructure cybersecurity remains characterized by deep structural fragmentation and regulatory incoherence, creating significant barriers to the effective implementation of emerging legal norms. National and sectoral laws differ widely in scope, terminology, enforcement mechanisms, and compliance expectations, producing an inconsistent governance environment in which operators of essential services must navigate divergent frameworks. Some jurisdictions rely primarily on voluntary guidelines inspired by soft-law instruments, while others impose binding statutory obligations, resulting in uneven levels of protection across sectors and regions. Comparative analyses of institutional cybersecurity design highlight how the absence of harmonized regulatory standards allows vulnerabilities to persist, particularly in states where administrative capacities remain underdeveloped or fragmented among multiple agencies (Savchuk, 2023). The diversification of governance models across the energy, healthcare, transportation, and financial sectors compounds this problem, as each sector independently interprets risk thresholds and compliance norms, creating incoherence that adversaries can exploit. Legal studies examining national infrastructure investment policies similarly demonstrate that institutional fragmentation reduces the ability of governments to ensure consistent protections across interconnected systems, undermining resilience efforts at the structural level (Zatonatskiy & Lavrentiev, 2023). As cyber threats increasingly target cross-sector dependencies, regulatory inconsistency has become one of the most significant weaknesses in the global cybersecurity governance regime.

The gap between formal legal mandates and the operational capacity of industry to implement them presents a second major enforcement challenge. Even when states adopt robust statutory obligations, operators of critical infrastructure may lack the technical expertise, financial resources, or organizational maturity necessary to meet demanding regulatory standards. Studies on information security maturity within public-sector institutions reveal that capacity constraints are widespread, particularly in systems that rely on outdated operational technologies or are undergoing digital transformation without adequate investment in security controls (Hochstetter et al., 2023). In the healthcare sector, research examining hospitals' legal responsibilities after the global pandemic shows that institutions often struggle to meet cybersecurity expectations despite legal obligations to protect patient rights and system availability, illustrating how regulatory mandates may exceed practical feasibility (Irawati, 2023). Financial infrastructure, similarly, faces challenges in adapting to new regulatory obligations associated with digital currency systems and modernized payment infrastructures, as operators must not only comply with new cryptographic and operational standards but also ensure backward compatibility and operational continuity (Bakhtiyar et al., 2023). This tension between legal expectation and operational reality reveals a systemic gap in cybersecurity governance: the existence of laws

does not guarantee their enforceability. Without capacity-building policies that support compliance, legal obligations remain aspirational rather than transformative.

Weak enforcement mechanisms further exacerbate these governance challenges, as many states lack the institutional structures necessary to conduct oversight, perform audits, and impose sanctions on operators that neglect cybersecurity requirements. Some regulatory frameworks rely heavily on voluntary compliance without meaningful penalties for non-adherence, limiting their ability to create behavioral change. Analyses of African cybersecurity policy frameworks demonstrate that insufficient enforcement authority and resource limitations within national agencies prevent governments from effectively overseeing critical infrastructure operators, resulting in gaps between formal legal obligations and actual security practices (Orji, 2022). Similarly, critiques of environmental regulatory governance reveal how the absence of meaningful monitoring systems allows regulated entities to underperform without consequence, highlighting the broader challenge of reliance on self-reporting and discretionary compliance (S., 2023). In the cybersecurity context, inadequate enforcement mechanisms not only weaken regulatory effectiveness but also reduce incentives for private-sector investment in preventive measures, as operators may calculate that non-compliance entails minimal legal risk. This structural weakness undermines the normative shift toward binding cybersecurity obligations by eroding the credibility of enforcement regimes.

Cross-border enforcement challenges represent another structural barrier to effective governance, given that critical infrastructure increasingly depends on transnational data flows, distributed digital service providers, and multinational supply chains. Jurisdictional overlaps and conflicts between national laws complicate the ability of regulators to investigate incidents, impose penalties, or compel cooperation from foreign entities involved in infrastructure operations. Studies examining coordinated threat intelligence frameworks emphasize that data sovereignty concerns often hinder real-time information sharing, as states prioritize national control over data at the expense of cross-border cooperation (Ndubuisi, 2023). Legal analyses of nation-state cyber operations demonstrate that states frequently exploit jurisdictional fragmentation by conducting operations from territories less subject to international scrutiny, complicating attribution and enforcement efforts (Tiwari, 2022). The absence of harmonized international legal obligations specifically addressing critical infrastructure protection further deepens these gaps, as existing treaties focus primarily on cybercrime rather than infrastructure resilience. Without a unified global governance structure, enforcement remains constrained by national boundaries that do not reflect the distributed nature of modern cyber operations.

Attributing cyberattacks poses additional challenges that directly impact enforcement, accountability, and deterrence. Cyberattacks on critical infrastructure often involve sophisticated obfuscation techniques, including proxy servers, false-flag operations, anonymization tools, and compromised third-party systems. Research on international cyber operations highlights that attribution remains one of the most contentious and uncertain aspects of cyber governance, as technical evidence alone is rarely sufficient to meet legal thresholds for state responsibility (Tiwari, 2022). This ambiguity hampers the ability of states to pursue legal remedies, impose sanctions, or take countermeasures consistent with international law. At the domestic level, attribution uncertainty limits regulators' capacity to identify negligent practices or assign responsibility when incidents occur. Institutional analyses of state cybersecurity policy emphasize that without clear attribution mechanisms, enforcement agencies cannot effectively determine whether failures stem from inadequate private-sector security practices or malicious external activity (Savchuk, 2023). The resulting ambiguity undermines deterrence, as adversaries may perceive a low likelihood of meaningful consequences for their actions.

The tension between state responsibility and private-sector accountability also complicates enforcement, particularly in jurisdictions where critical infrastructure is owned or operated by private entities. Many legal frameworks impose obligations on private providers while simultaneously relying on them to implement national security directives, creating ambiguous boundaries between corporate responsibility and state authority. Research examining national cybersecurity strategies highlights how this ambiguous division of responsibility can create compliance gaps, as operators may perceive certain obligations as governmental duties rather than business requirements (Adegbite et al., 2023). Administrative law analyses further reveal that enforcement agencies sometimes lack the legal authority to compel private operators to implement stringent protective measures, especially in sectors where privatization has limited state control over operational decisions (Макарчук, 2021). These tensions undermine coordinated security efforts, as neither public nor private actors may possess a clear

understanding of their respective enforcement responsibilities, resulting in inconsistent implementation of cybersecurity obligations.

Supply chain vulnerabilities represent another critical gap in enforcement, as existing regulatory frameworks often fail to fully account for risks arising from third-party service providers, hardware manufacturers, and software vendors. Research on infrastructure project financing demonstrates that complex contractual arrangements can obscure accountability when security failures originate from external partners (Nathaniel et al., 2022). Similarly, studies analyzing digital financial infrastructure highlight how risks embedded in vendor technologies or distributed operational systems can produce cascading failures across national economies (Bakhtiyar et al., 2023). Yet, many cybersecurity regulations do not impose explicit obligations for continuous monitoring, auditing, or certification of third-party security practices, allowing vulnerabilities to persist in opaque vendor ecosystems. Even when supply chain requirements exist, enforcement frequently remains limited due to inadequate auditing capacities or insufficient access to proprietary vendor information. These gaps expose critical infrastructure to infiltration through upstream vulnerabilities that operators may not detect or control.

Another systemic challenge arises from the paradox of national security secrecy, which can unintentionally reduce transparency and limit external scrutiny of cybersecurity compliance. To protect sensitive operational details, states often restrict access to information about security practices, incident reports, and vulnerabilities. While such secrecy may be necessary for preventing adversarial exploitation, it also limits the ability of civil society, independent auditors, and even other government agencies to evaluate the adequacy of compliance efforts. National security analyses highlight that over-classification and secrecy norms can undermine institutional accountability by preventing oversight bodies from obtaining the information necessary to assess regulatory effectiveness (Макарчук, 2021). In the private sector, nondisclosure agreements and confidentiality policies similarly restrict the disclosure of breaches or vulnerabilities, preventing broader learning and weakening collective resilience. This tension between secrecy and accountability creates blind spots in enforcement, allowing vulnerabilities to remain unaddressed and complicating efforts to assess compliance across interconnected systems.

These structural, legal, institutional, and practical gaps illustrate why existing cybersecurity norms, despite their evolution toward mandatory obligations, remain insufficient to ensure robust protection of critical infrastructure. Fragmented laws create inconsistent obligations, capacity gaps limit implementation, weak enforcement mechanisms undermine compliance, cross-border complexities impede legal remedies, attribution challenges reduce accountability, public–private tensions obscure responsibility, supply chain vulnerabilities escape regulatory scrutiny, and secrecy norms restrict oversight. Together, these systemic issues reveal a governance architecture that is still misaligned with the operational realities of contemporary cyber threats, highlighting the urgent need for more coherent, coordinated, and enforceable frameworks capable of addressing the multi-dimensional nature of critical infrastructure cybersecurity.

5. Conclusion

The evolving landscape of critical infrastructure cybersecurity reveals a governance environment marked by both significant progress and persistent structural challenges. As states confront an increasingly hostile cyber domain, legal and regulatory frameworks have undergone a notable transformation, shifting from voluntary standards toward more binding and enforceable obligations. This shift reflects a growing recognition that essential services cannot depend solely on discretionary guidance or fragmented self-regulation, particularly as cyber threats continue to diversify, intensify, and acquire geopolitical significance. Yet, even as legal norms advance toward greater institutionalization, the broader governance architecture remains fundamentally incomplete. The fragmentation of national policies, the unevenness of sectoral frameworks, and the continued dominance of soft-law instruments in many jurisdictions all contribute to an inconsistent global system that struggles to keep pace with technological and adversarial evolution.

A central challenge lies in bridging the gap between legal mandates and operational realities. Critical infrastructure operators, particularly in sectors marked by rapid digital transformation, often face significant resource constraints that limit their capacity to comply with sophisticated regulatory requirements. Legacy technologies, limited cybersecurity expertise, and budgetary pressures frequently impede the practical implementation of mandated security controls. Without parallel investments in capacity building, workforce development, and modernization of operational technologies, the conversion of

norms into enforceable obligations risks becoming performative rather than substantive. The result is a regulatory environment where expectations may rise, but actual resilience remains uneven, creating vulnerabilities that adversaries can exploit.

The effectiveness of any cybersecurity framework ultimately depends on enforcement, yet this remains one of the weakest dimensions of global governance. Many states lack the institutional capacities required to conduct audits, monitor compliance, and impose meaningful penalties for violations. Even in jurisdictions with strong regulatory mandates, enforcement bodies may struggle with jurisdictional limitations, resource constraints, or insufficient coordination among agencies. In sectors dominated by private ownership, state authorities often depend on voluntary cooperation from operators, creating additional obstacles to rigorous oversight. The absence of strong enforcement mechanisms minimizes the deterrent effect of regulations and weakens the incentive for organizations to prioritize proactive cybersecurity investments.

Cross-border complexities further complicate governance. Critical infrastructure increasingly depends on global supply chains, distributed computing environments, and international data flows, making it difficult for any single state to ensure comprehensive protection. Jurisdictional overlaps and conflicts impede cooperation, while varying regulatory standards across countries create gaps where attackers can operate with relative impunity. International frameworks, although improving, remain limited in scope and often lack the binding force needed to address the transnational nature of cyber threats. Without harmonized global standards and improved mechanisms for international collaboration, enforcement will continue to be hampered by legal and territorial fragmentation.

Attribution remains a defining challenge in cybersecurity governance. The technical complexity of modern cyber operations allows attackers to obfuscate their identities, route attacks through compromised systems, and engineer false-flag operations that mislead investigators. In the absence of reliable attribution, assigning responsibility becomes fraught with uncertainty, undermining both domestic legal accountability and international deterrence. As critical infrastructure increasingly becomes a target of state-aligned and criminal actors alike, the inability to consistently identify perpetrators limits the effectiveness of punitive and corrective measures. This uncertainty contributes to an environment where legal obligations exist but may be rendered ineffective by practical barriers to enforcement.

Tensions between state and private-sector responsibilities further undermine the governance landscape. With much critical infrastructure operated by private or semi-private entities, determining the boundary between public obligations and private duties is often unclear. States may impose stringent requirements without providing adequate guidance or support, while private operators may assume that certain responsibilities lie primarily with national authorities. This ambiguity creates gaps in implementation, reduces accountability, and complicates coordinated responses to emerging threats. Building effective governance structures requires clearer delineation of roles, improved communication channels, and shared responsibility frameworks that align incentives across public and private actors.

Supply chain vulnerabilities highlight yet another persistent gap. Modern infrastructure ecosystems rely on diverse external vendors, cloud providers, and hardware manufacturers, many of which operate beyond the jurisdiction or oversight of national regulators. Security flaws or malicious insertions in upstream components can compromise entire networks, yet many regulatory frameworks still lack comprehensive requirements for supply chain risk management. Even when requirements exist, enforcement remains difficult due to limited auditing capabilities and the proprietary nature of vendor technologies. As global supply chains grow more complex and interconnected, addressing these vulnerabilities will require legal frameworks that extend beyond primary operators and encompass the full lifecycle of digital infrastructure components.

Compounding these challenges is the paradox inherent in national security secrecy. Governments often restrict disclosure of cybersecurity vulnerabilities, incident details, and compliance assessments in the name of national defense. While such secrecy may prevent adversaries from exploiting sensitive information, it also reduces transparency, weakens oversight, and prevents the broader ecosystem from learning from incidents. Without adequate visibility into the state of infrastructure security, policymakers, independent auditors, and even other government agencies may struggle to evaluate the effectiveness of existing laws and regulations. Balancing national security confidentiality with the need for accountability remains one of the most delicate governance dilemmas in the cybersecurity domain.

Taken together, these issues reveal a cybersecurity governance environment that is evolving but still insufficient to meet the scale and complexity of contemporary threats. Emerging legal norms represent meaningful progress, signaling a shift toward greater institutional responsibility, enhanced accountability, and more structured protective frameworks. However, legal evolution alone cannot compensate for persistent enforcement gaps, capacity limitations, jurisdictional fragmentation, and the

inherent challenges of attributing and responding to cyberattacks. Ensuring the security and resilience of critical infrastructure requires not only robust laws but integrated institutional architectures capable of operationalizing them.

Future progress will depend on building stronger enforcement mechanisms, expanding regulatory capacity, and harmonizing cross-border obligations. It will also require fostering closer public–private cooperation, improving supply chain transparency, and investing in technological innovation that aligns with emerging security standards. Most importantly, governance systems must adapt to the dynamic nature of cyber threats by embracing flexibility, responsiveness, and continuous improvement. Only through coherent, coordinated, and forward-looking approaches can states ensure that critical infrastructure remains secure in an increasingly unpredictable digital environment.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all participants who participate in this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Adegbite, A. O., Akinwolemiwa, D. I., Uwaoma, P. U., Kaggwa, S., Akindote, O. J., & Dawodu, S. O. (2023). Review of Cybersecurity Strategies in Protecting National Infrastructure: Perspectives From the Usa. *Computer Science & It Research Journal*, *4*(3), 200-219. https://doi.org/10.51594/csitrj.v4i3.658

Bakhtiyar, A. C., Rosadi, S. D., & Handayani, T. (2023). Juridical Studies of the Legal Status of Digital Rupiah in the Context of Modernizing Financial Market Infrastructure. *Jurnal Poros Hukum Padjadjaran*, *5*(1), 53-70. https://doi.org/10.23920/jphp.v5i1.1423

Hochstetter, J., Diéguez, M., Fenner, J. L., & Cachero, C. (2023). AIM Triad: A Prioritization Strategy for Public Institutions to Improve Information Security Maturity. *Applied Sciences*, *13*(14), 8339. https://doi.org/10.3390/app13148339

Irawati, J. (2023). Judicial Review of Hospitals' Legal Responsibility of Patients' Rights After the Covid-19 Pandemic. *Law Review*, *23*(1), 16. https://doi.org/10.19166/lr.v23i1.6892

Kashyap, A. K., & Chaudhary, M. P. (2023). Cyber Security Laws and Safety in E-Commerce in India. *Law and Safety*, *89*(2), 207-216. https://doi.org/10.32631/pb.2023.2.19

Malone, M., & Walton, R. (2023). Comparing Canada's Proposed Critical Cyber Systems Protection Act With Cybersecurity Legal Requirements in the EU. *International Cybersecurity Law Review*, *4*(2), 165-196. https://doi.org/10.1365/s43439-023-00082-1

Nathaniel, A. W. J., Dewi, Y. K., & Sani, S. D. (2022). Third-Party Risk in the Availability Payment: The Palapa Ring Western Package. *Journal of Indonesian Legal Studies*, *7*(1), 339-390. https://doi.org/10.15294/jils.v7i1.55184

Ndubuisi, A. F. (2023). Strengthening National Cybersecurity Policies Through Coordinated Threat Intelligence Sharing and Real-Time Public-Private Collaboration Frameworks. *International Journal of Science and Research Archive*, *8*(2), 812-831. https://doi.org/10.30574/ijsra.2023.8.2.0299

Oluoha, O. M., Odeshina, A., Reis, O., Okpeke, F., Attipoe, V., & Orieno, O. H. (2022). Artificial Intelligence Integration in Regulatory Compliance: A Strategic Model for Cybersecurity Enhancement. *Ijfmr*, *3*(1), 35-46. https://doi.org/10.54660/.ijfmr.2022.3.1.35-46

Orji, U. J. (2022). Interrogating African Positions on State Sponsored Cyber Operations: A Review of Regional and National Policies and Legal Responses. *Baltic Yearbook of International Law Online*, *20*(1), 236-267. https://doi.org/10.1163/22115897_02001_012

S., S. (2023). Assessing the Impact of Environmental Policy, 2006: A Critical Examination. *International Journal for Multidisciplinary Research*, *5*(5). https://doi.org/10.36948/ijfmr.2023.v05i05.6179

Savchuk, S. B. (2023). Institutional and Legal Model for the Formation and Implementation of the State Policy of Combating Cybercrime. *Public Policy and Accounting*(2(8)), 56-60. https://doi.org/10.26642/ppa-2023-2(8)-56-60

Takuro, K. O. (2023). Exploring Cybersecurity Law Evolution in Safeguarding Critical Infrastructure Against Ransomware, State-Sponsored Attacks, and Emerging Quantum Threats. *International Journal of Science and Research Archive*, *10*(2), 1518-1535. https://doi.org/10.30574/ijsra.2023.10.2.1019

Thumfart, J. (2022). The (Il)legitimacy Of Cybersecurity. An Application Of Just Securitization Theory To Cybersecurity Based On The Principle of Subsidiarity. *Applied Cybersecurity & Internet Governance*, *1*(1), 1-24. https://doi.org/10.5604/01.3001.0016.1093

Tiwari, S. (2022). Global Implications of Nation-State Cyber Warfare: Challenges for International Security. *Ijrmeet*, *10*(3), 42-61. https://doi.org/10.63345/ijrmeet.org.v10.i3.6

Zatonatskiy, D., & Lavrentiev, M. (2023). Institutional Support for Investing in Critical Infrastructure Objects in Ukraine. *1*, 149-163. https://doi.org/10.61432/cpne0101149z

Zhyvylo, E. O., & Shevchenko, D. (2022). Risk Assessment of Cyber Security and Control of Privacy in Public Administration Information Systems. *Collection of Scientific Works of the Military Institute of Kyiv National Taras Shevchenko University*(75), 66-77. https://doi.org/10.17721/2519-481x/2022/75-07

Макарчук, В. В. (2021). Administrative and Legal Status of Law Enforcement Bodies as Subjects of Formation and Implementation of State Policy in the Field of National Security and Defense. *Law Journal of Donbass*, *75*(2), 35-44. https://doi.org/10.32366/2523-4269-2021-75-2-35-44