Applied Science, Computing and Energy, 2025, 3(3), 512-537

A Strategic Framework for Strengthening Cyber Risk Governance and Resilience in US Critical Infrastructure Sectors

Aman Shrestha
Received:27 June 2025/Accepted: 02 October 2025/Published:25 October 2025
Email: shrestha524951@avila.edu

Abstract: *This paper presents a comprehensive approach to the strategic governance and resilience of cyber risk in the US critical infrastructure sectors. With threats such as the 2021 Colonial Pipeline ransomware attack, which disrupted fuel supply and caused economic and social chaos, strong governance is vital. The current study employs resilience theory, risk management, and governance models to develop a solution for protecting critical infrastructure amid evolving threats. The framework includes four pillars: adaptive governance, real-time threat intelligence, cross-sector collaboration, and resilience building. By examining existing frameworks, regulations, and sector weaknesses, key gaps are identified, leading to potential improvements suggested. Results show that effective cyber risk governance should move beyond compliance to dynamic, intelligence-led models that emphasize rapid adaptation, stakeholder coordination, and capability development. This framework provides practical guidance for policymakers, operators, and cybersecurity experts to strengthen national resilience against cyber threats. These implications are intended to inform future policy-making, enhance relations between the populace and the private sector, and improve the security landscape of critical infrastructure sectors essential to national security and economic stability.*

Keywords*: Cyber risk, infrastructure protection, cybersecurity strategy, threat intelligence, risk management*

Aman Shrestha
School of Computer Science & Mathematics. Avila University, 11901 Wornall Rd, Kansas City, MO 64145. USA.

1.0 Introduction

The digitalization of critical infrastructure has radically shifted the risk environment in modern societies. What used to be a remote operational technology infrastructure has become a very interconnected network, in which a failure in one sector can trigger a domino effect in many areas (Moteff and Parfomak, 2015). On May 7, 2021, the Colonial Pipeline, which transports 45% of the fuel used on the East Coast, was targeted by the Darkside ransomware group, triggering fuel shortages and an emergency declaration in 17 states (Turton and Mehrotra, 2021). This event highlighted a disturbing reality: even after spending billions on cybersecurity, the governance systems that safeguard America's most critical systems remain disjointed, reactive, and poorly aligned.

Beyond the immediate operational and economic consequences of cyber incidents, the governance of cyber risk in critical infrastructure is increasingly understood through the lens of resilience theory and complex adaptive systems. Critical infrastructure sectors function as socio-technical systems in which technological assets, human operators, institutional rules, and market forces interact dynamically. Resilience in this context extends beyond prevention to encompass the ability to anticipate, absorb, recover from, and adapt to cyber disruptions. Scholars argue that governance structures must therefore be adaptive, learning-oriented, and capable of responding to uncertainty rather than relying solely on static control mechanisms or perimeter-based defenses (Linkov et al., 2019; Woods, 2015).

Cyberattacks on critical infrastructure rose 87% from 2019 to 2024, with threat actors

increasingly breaching critical services (CISA, 2024). In 2021, the largest meat processor, JBS Foods, was breached, while attackers also easily targeted the Oldsmar water treatment to alter water chemicals (Perlroth, 2021). In 2023, healthcare systems faced over 1,400 breaches, disrupting medical services and record security (HHS, 2024).

These attacks reveal systemic flaws in both technical defenses and governance frameworks for predicting, stopping, and mitigating cyber threats. Current strategies are mostly compliance-based, with minimal efforts to build resilience. The rise of industry-specific systems creates isolated protections that overlook the interdependence of modern infrastructure (Hathaway and Klimburg, 2023). Asymmetries between defenders and attackers exacerbate the issue: operators must patch all vulnerabilities, while adversaries need only find one. Nation-states have gained access to critical networks, enabling persistent spying and attack preparation (NSA, 2023).

Current governance systems struggle with dynamic threats and inadequate policy strategies. The NIST Cybersecurity Framework offers guidance and strengthen policy solutions but is limited by voluntary implementation and broad applicability, hindering behavioral change (NIST, 2024; Siame, 2025). CISA has limited authority to enforce security outside federal systems (CISA, 2021). Regulatory hurdles exist as 85% of critical infrastructure is privately owned (DHS, 2022). Despite laws, information sharing remains difficult due to companies' reluctance to share vulnerability or breach information (Chowdhury and Gkioulos, 2019).

The only noticeable omission is an integrated strategic approach that moves beyond piecemeal methods. This paper addresses that gap by proposing a holistic strategic framework aimed at improving cyber risk governance and resilience within key infrastructure sectors in the US. The study has three interconnected goals: first, it reviews current theoretical insights and empirical data to establish a solid foundation for understanding cyber risk governance issues; second, it develops a comprehensive system built on four essential pillars to bridge gaps in existing approaches; third, it offers practical insights into implementation mechanisms and industry-specific adjustments that help turn abstract principles into actionable guidance for policymakers, regulators, and infrastructure operators.

1.1 Theoretical Framework

To understand cyber risk governance of critical infrastructure, one must engage with various theoretical traditions. Our framework rests on three main pillars: resilience theory, risk governance theory, and organizational learning theory.

The term 'resilience' has become the dominant framework for protecting critical infrastructure, though it has multiple meanings (Linkov and Palma-Oliveira, 2014). Engineering resilience focuses on quickly restoring systems to their pre-disturbance state, while ecological resilience emphasizes adaptive capacity, the ability to reorganize systems and maintain vital functions amid changing conditions (Holling, 1973). This distinction is especially significant in cybersecurity. The resilience cycle comprises four key stages: anticipation, which involves threat scanning and identifying vulnerabilities; absorption, which means enduring disruptions through redundancy and robust design; adaptation, which entails modifying operations during and after an incident; and recovery, which involves restoring functionality and learning from the experience (Linkov et al., 2013).

Risk governance theory complements resilience thinking by focusing on the institutional structures through which societies recognize, assess, and respond to risks (Renn and Walker, 2011). Unlike traditional risk management, which assumes a designated decision-maker, risk governance recognizes that modern risks

often cross borders—affecting countries, industries, and diverse stakeholders. Effective governance requires coordinating actions among various actors and managing conflicts arising from incompatible values (Aven and Renn, 2016). The perception of risk becomes especially important, as technical experts often assess risks differently than the general society (Slovic, 1987).

Organizational learning theory explains how organizations develop their capacity over time (Argyris and Scho¨n, 1978). Single-loop learning involves identifying and correcting errors within existing assumptions, while double-loop learning questions those assumptions and can lead to changes in organizational strategies (Senge, 1990). In cybersecurity, communities of practice play a crucial role as they facilitate ongoing knowledge creation to keep pace with rapidly evolving threats (Wenger, 1998).

The NIST Cybersecurity Framework has seen widespread adoption due to its user-friendly structure, which organizes cybersecurity activities into five core functions: Identify, Protect, Detect, Respond, and Recover (NIST, 2024). However, there are limitations to protecting critical infrastructure. Its voluntary nature has contributed to broad adoption, yet it provides limited guidance on the cross-organizational coordination needed to support interconnected infrastructure (Hathaway and Klimburg, 2023). Additional methods are offered through international standards such as ISO/IEC 27001 and IEC 62443 (ISO, 2013). Although sector-specific regulations, including the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards for the energy sector and the Health Insurance Portability and Accountability Act (HIPAA) requirements for the healthcare sector, provide more detailed and enforceable controls, they further complicate the governance landscape by introducing fragmented, sector-bound compliance regimes that are often misaligned with the interconnected nature of critical infrastructure systems (IEC, 2018). As a result, organizations operating across multiple sectors or supply chains must navigate overlapping and sometimes conflicting regulatory expectations, which can hinder information sharing, slow coordinated response efforts, and ultimately weaken system-wide cyber resilience.

The federal policy environment has undergone significant change. Presidential Policy 21 identified critical infrastructure sectors and designated Sector Risk Management Agencies (Obama, 2013). The 2015 Cybersecurity Information Sharing Act provided a legal basis for sharing information (Congress, 2015), while the 2018 Cybersecurity and Infrastructure Security Agency Act established CISA within DHS (Congress, 2018). Additionally, Executive Order 14028 mandated security protocols for federal agencies following high-profile attacks (Biden, 2021).

Despite these efforts, significant gaps remain. Interoperability between frameworks is limited, and organizations face conflicting requirements from various regulatory systems. Existing solutions lack adaptive governance capable of quickly responding to threats. The private sector's participation incentives are weak, and resilience assessment measures are still under development.

Fig. 1 displays 16 critical infrastructure sectors identified by CISA, connected by lines showing interdependencies, such as energy's reliance on IT and communications, healthcare on water and energy, and finance on communications.

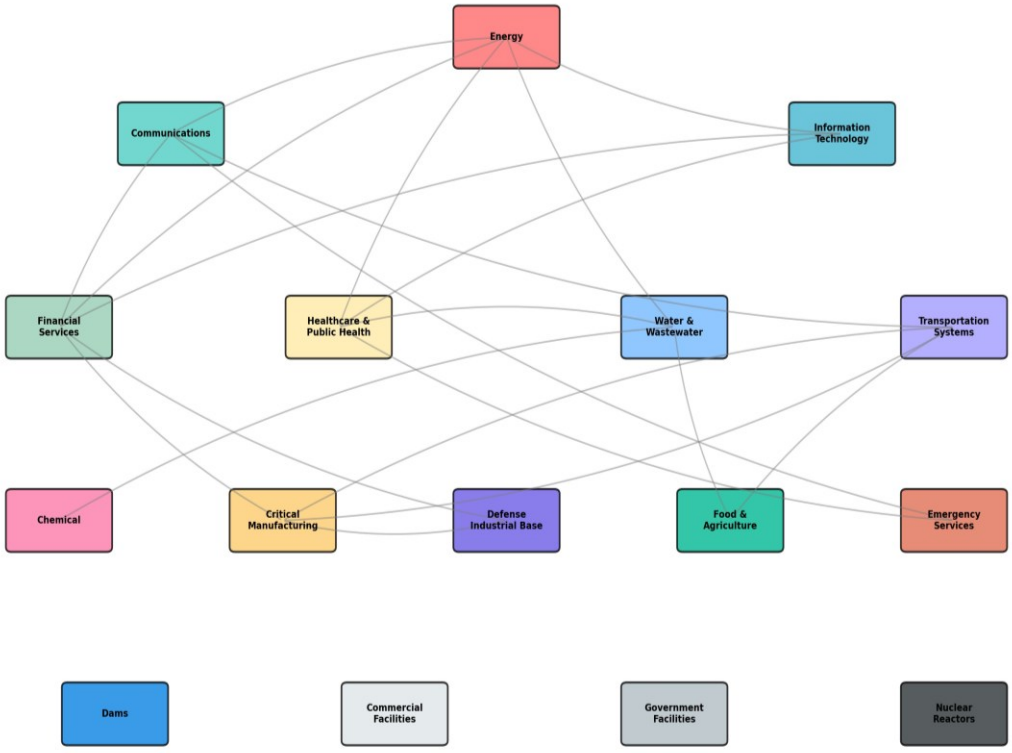
2.0 Materials and Method

Creating a strategic framework for cyber risk governance requires a methodology that can synthesize empirical insights from diverse sources. This study employed a combination of systematic literature review, expert consultation, a comparison framework, and case analysis to develop a comprehensive and practical framework. The research followed design science principles (Hevner

et al., 2004; Siame et al., 2023), focusing on creating a new artifact rather than testing hypotheses about existing phenomena. The goal is for the framework to effectively address real-world problems, be feasible for implementation, and surpass current methods (March and Smith, 1995).

Table 1 is introduced to provide a structured comparison of the major cybersecurity frameworks currently applied to the protection of critical infrastructure in the United States and internationally. As discussed in the preceding sections, the governance landscape for critical infrastructure cybersecurity is highly fragmented, with organizations often required to comply with multiple frameworks that differ in scope, enforceability, and operational focus. Table 1 summarizes these frameworks by outlining their scope, key strengths, limitations, and primary drivers of adoption, thereby offering a concise overview of how existing approaches shape cyber risk governance across sectors.

As shown in Table 1, widely adopted frameworks such as the NIST Cybersecurity Framework and ISO/IEC 27001 emphasize flexibility and broad applicability, which has supported widespread uptake but has also limited their ability to enforce consistent security behaviors across interconnected sectors. Sector-specific and mandatory standards, such as NERC CIP for the electric sector and the HIPAA Security Rule for healthcare, provide clearer accountability and enforceable controls, yet they tend to be compliance-focused and narrowly scoped, reducing adaptability to evolving threats and cross-sector interdependencies. The comparison highlights a central governance challenge addressed by this study: while existing frameworks provide valuable guidance, none alone adequately support adaptive, intelligence-led, and system-wide resilience. This gap underscores the need for an integrated strategic framework that aligns governance structures, real-time threat intelligence, and resilience-building mechanisms across critical infrastructure sectors.



Fig, 1: US Critical Infrastructure Sectors and Their Interdependencies.

Table 1: Comparison of Major Cybersecurity Frameworks for Critical Infrastructure

Framework	Scope	Key Strengths	Limitations	Adoption Drivers
NIST CSF	Cross-sector, voluntary	Flexible, outcomefocused, widely recognized	Limited enforcement, generic guidance	Regulatory expectations, customer requirements
ISO/IEC 27001	International standard	Comprehensive certification available	Resource-intensive, documentation-heavy	Market differentiation, contractual requirements
IEC 62443	Industrial control systems	OT-specific, safetyintegrated	Complex implementation, evolving standard	Operational technology security needs
NERC CIP	Electric sector, mandatory	Enforceable, specific controls	Compliancefocused, limited flexibility	Regulatory compliance, financial penalties
HIPAA Security Rule	Healthcare sector	Privacy-integrated, baseline requirements	Outdated, insufficient for current threats	Legal compliance, patient trust

3.0`Results and Discussion

Our initial step involved conducting a systematic review of academic papers, policy reports, and industry publications from 2015 to 2025. This period includes major events such as the 2015 power grid attack in Ukraine, the 2017 NotPetya malware outbreak, and ransomware attacks on critical infrastructure that began in 2019 (Greenberg, 2019). Literature searches were performed across multiple databases, including Scopus, Web of Science, IEEE Xplore, ACM Digital Library, and Google Scholar. An initial search yielded over 1,200 potentially relevant sources, which were then screened for relevancy. Ultimately, 276 sources were selected for detailed review, with thematic analysis employed to identify key themes, tensions, and gaps. These findings provided an empirical foundation for assessing governance maturity, identifying systemic weaknesses, and informing the design of the proposed strategic framework.

The literature review was complemented by expert consultations that incorporated tacit knowledge. We conducted semi-structured interviews with 27 cybersecurity experts, including eight federal government officials, 12 CISOs and security directors from the private sector, four academic researchers, and three cybersecurity consultants. The interviews addressed current governance practices, the perceived benefits and drawbacks of existing frameworks, obstacles to effective governance, experiences with information sharing, significant incidents and lessons learned, and potential improvements. Across sectors, experts consistently emphasized that governance fragmentation, delayed information sharing, and unclear accountability structures were more limiting than purely technical security deficiencies

The case studies analyzed real-world examples of governance successes and failures. We examined five major

cyberattacks, including the Colonial Pipeline ransomware attack (2021), the JBS Foods attack (2021), the Oldsmar water treatment facility intrusion (2021), COVID-19-related healthcare ransomware incidents (2020-2021), and the SolarWinds supply chain breach (2020). Additionally, we compared governance approaches, focusing on the European Union's NIS2 Directive, the United Kingdom's National Cyber Security Strategy, and Australia's Critical Infrastructure Protection legislation.

The development of the frameworks was driven by ongoing discussions that integrated theoretical knowledge, factual information, professional insights, case studies, and global practices. Validation involved multiple methods, including two rounds of Delphi with fifteen experts, presentations at practitioner conferences, and evaluations by CISOs from three companies with critical infrastructure.

3.1 Current State Assessment

The modern threat landscape reflects the democratization of advanced attack methods and the rise of state-sponsored operations. Ransomware attacks are the most common immediate threat, with their prevalence in critical infrastructure rising threefold from 2019 to 2023 (FBI, 2024). APT actors from China, Russia, Iran, and North Korea have maintained persistent campaigns targeting critical infrastructure networks (Mandiant, 2023). The SolarWinds breach highlighted how supply chain attacks can compromise numerous targets simultaneously (Gallagher, 2020), while the Volt Typhoon operation specifically targeted US critical infrastructure operational technology networks (CISA, 2023).

We reviewed governance maturity across industries, revealing significant variation. Using a five-level maturity model based on CMMI (CMMI, 2010), the most mature sectors are financial services and the defense industrial base, both of which are subject to strict regulation. Energy and communications are moderately highly mature. Conversely, healthcare, water/wastewater, and food/agriculture tend to be less mature, mainly due to resource constraints and minimal regulatory requirements.

Table 2 is presented to extend the comparative analysis by focusing on the operational and technical mechanisms through which cybersecurity resilience is implemented across critical infrastructure sectors. While Table 1 emphasizes governance structures and regulatory frameworks, Table 2 shifts attention to the practical tools, technologies, and processes that organizations deploy to detect, prevent, respond to, and recover from cyber incidents. This distinction is important because effective cybersecurity in critical infrastructure depends not only on compliance with frameworks, but also on how technical controls and operational practices are integrated into day-to-day system operations.

As summarized in Table 2, preventive controls such as network segmentation, access control, and secure system architecture form the first line of defense, but their effectiveness is highly dependent on sector-specific operational constraints and legacy infrastructure. Detection and response mechanisms—including intrusion detection systems, security information and event management (SIEM), and incident response protocols—are shown to play a critical role in limiting the impact of attacks, particularly in environments where real-time operations and safety considerations restrict system downtime. The table also highlights disparities in maturity across sectors, with energy and finance generally exhibiting more advanced monitoring and response capabilities than water, transportation, and healthcare systems. Overall, Table 2 reinforces the study’s argument that technical controls must be tightly aligned with governance frameworks and risk management strategies to achieve adaptive, system-wide cyber resilience across interconnected critical infrastructure networks.

3.1 The Strategic Framework: Core Components

Our strategic framework rests on four interconnected pillars, each addressing different but related governance challenges.

Pillar 1: Adaptive Governance Structures recognizes that static governance models cannot keep pace with rapidly evolving cyber threats. Effective governance should incorporate continuous learning mechanisms, regular reviews, and swift adaptability. This pillar emphasizes dynamic policy tools, such as sunset clauses that require periodic policy re-evaluation

Table 2: Critical Infrastructure Sectors- Threat Profile and Governance Maturity Matrix.

Sector	Primary Threats	Key Vulnerabilities	Maturity Level	Governance Gaps
Energy	State actors, ransomware, physicalcyber convergence	Legacy SCADA, supply chain, remote ac-cess	High (Tier 3-4)	Small operator coverage, OT-IT integration
FinancialSer-vices	State actors, organized crime, insider threats	Third-party dependencies, data aggregation	Very High (Tier 4)	Cross-border coordination, fintech integration
Healthcare	Ransomware, data breaches, medical device attacks	Resource constraints, legacy devices, fragmentation	Low-Moderate (Tier 2)	Small facility capacity, operational continuity emphasis
Transportation	State actors, ransomware, GPS/navigation threats	Physical-digital interfaces, legacy systems	Moderate (Tier 2-3)	Modal fragmentation, international coordination
Water Systems	Ransomware, state actors, SCADA in-trusions	Underfunding, small operator capacity, remote access	Low (Tier 1-2)	Resource limitations, distributed ownership

These flexible regulations and policy strategies prioritize results over strict rules, clear roles and responsibilities, and streamlined decision-making during crises (Siame et al., 2024). It also relies on regulatory sandboxes, similar to those used in financial technology regulation (Zetzsche et al., 2017; Akagbue et al., 2023; Siame et al., 2025), and the UK's model of outcome-based regulation combined with active engagement (NCSC, 2022). Pillar 2: Real-Time Threat Intelligence Integration deals with the core information asymmetry between the defenders of the infrastructure and the advanced adversaries. This pillar envisions an intelligence ecosystem in which actionable threat information is delivered to defenders as quickly as possible and in formats that can be used immediately. The main elements are automated threat detection and sharing systems, redesigned Information Sharing and Analysis Centers with more resources, the ability to bridge classified intelligence and unclassified operations, and predictive analytics using artificial intelligence. The pillar needs to overcome

the cultural and legal barriers to sharing information (Omosunlade, 2024; Sanni, 2024). The FS-ISAC of the financial industry illustrates the results of the continuous investment and executive involvement (FS-ISAC, 2023).

Pillar 3: Cross-Sector Collaboration Mechanisms recognizes that relationships within critical infrastructure mean sector security alone is insufficient for systemic resilience. The Colonial Pipeline attack disrupted transportation systems, impacting fuel supplies and supply chains across various fields. Achieving the necessary collaboration requires both horizontal coordination between sectors and vertical integration from federal to local levels. Such mechanisms include joint exercises to test cross-sector response, shared situational awareness during crises, mutual aid agreements for resource exchange, and Sector Coordinating Councils with clear protocols for rapid activation in emergencies (NATO, 2023).

Pillar 4: Resilience-Building Capabilities focuses on systematically developing institutional, technical, and human capacities essential for infrastructure resilience. Key aspects include strategic redundancy of critical systems, standards for rapid recovery to enable quick restorations, continuous capability testing through red team exercises and tabletop simulations, workforce preparedness to address the cybersecurity skills shortage, and channels for adopting innovative technologies. This pillar emphasizes that capability development is a long-term investment to be built gradually (DHS, 2023).

These four pillars do not operate in isolation; instead, they function synergistically. Adaptive governance creates dynamic systems essential for fostering successful cooperation. Intelligence integration enhances threat awareness, guiding governance decisions and priorities for capability development. Cross-sector cooperation enables sharing of information with intelligence agencies and helps identify common areas of need. Governance structures are valuable because they offer opportunities to build resilience and enable organizations to adopt necessary practices.

This integrated design ensures that improvements in one governance dimension reinforce progress in others, creating a cumulative effect on overall system resilience.

Fig. 4 illustrates the four pillars of the framework: Adaptive Governance Structures, Real-Time Threat Intelligence Integration, Cross-Sector Collaboration, and Resilience Building, connected to ensure critical infrastructure resilience. Arrows indicate interdependencies: adaptive governance facilitates collaboration, intelligence informs capability development, collaboration supports information sharing, and resilience aids governance adaptation. Theoretical foundations include resilience theory, risk governance, and organizational learning, while external factors such as the threat landscape, technological evolution, and policy context are depicted in the surrounding environment.

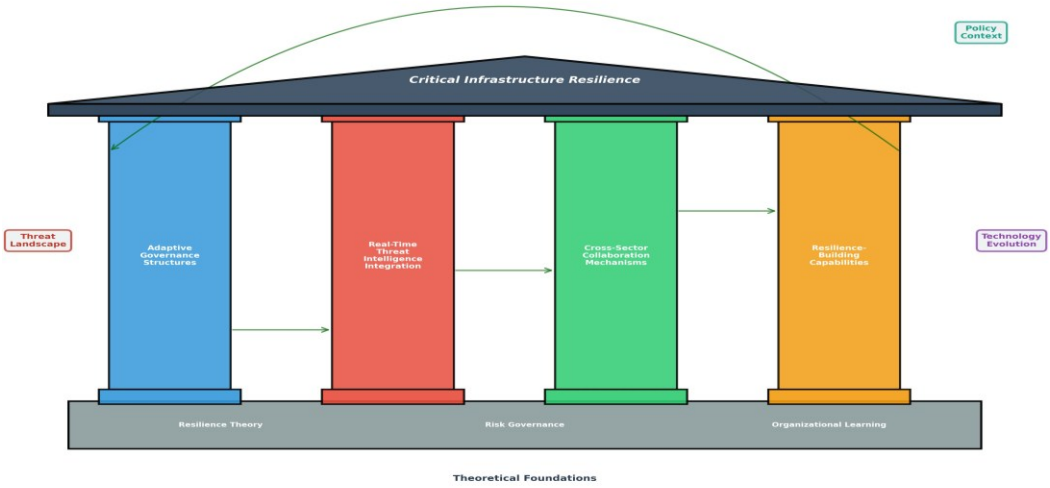


Fig. 2: The Strategic Framework Architecture, Four Pillars Integration Model.

3.2 Implementation Mechanisms

The translation of the abstract framework elements into operational practice must be implemented across three levels: governance, operational, and strategic. The governance level will establish national coordination arrangements in which CISA will have enhanced coordination provisions. The operational level focuses on daily security operations and incident response, particularly regarding information sharing and standard operating procedures. The strategic level involves long-term planning and resource allocation by defining priorities for capability development through multi-year plans. Sector-specific applications recognize that one size does not fit all practices. Implementing the framework in the energy industry should align with current NERC CIP requirements. In healthcare, implementation must address unique constraints such as the importance of patient safety and the security of medical devices. Fintech integration and global dependencies pose ongoing challenges to financial services. Transport systems are diverse in terms of modes of coordination and operational variations.

Table 3 presents the Sector-Specific Framework Customization Matrix, translating the strategic pillars of the cybersecurity framework into actionable priorities tailored to each critical infrastructure sector. While the overarching framework establishes adaptive governance, intelligence integration, collaboration, and resilience building, Table 3 emphasizes the operationalization of these principles according to sector-specific needs, acknowledging that each sector faces distinct threats, operational constraints, and regulatory requirements.

For the energy sector, the focus is on integrating operational technology (OT) and information technology (IT) systems, addressing supply chain vulnerabilities, and supporting smaller operators, with intelligence oriented toward state actor tactics and supply chain threats. Collaboration priorities highlight interdependent utilities and fuel supply coordination, while capabilities emphasize legacy system security and workforce training. The financial sector requires cross-border coordination, fintech regulation, and intelligence focused on fraud, ransomware, and advanced persistent threats, with collaboration extending to international partnerships and the vendor ecosystem; critical capabilities include quantum-safe cryptography and AI/ML-driven security measures. Healthcare prioritizes patient safety, medical device security, and support for smaller facilities, with intelligence aimed at healthcare-targeting ransomware and device vulnerabilities; collaboration focuses on hospital associations and device manufacturers, emphasizing basic

cybersecurity practices, segmentation, and recovery strategies. Transportation sectors face challenges related to modal coordination, GPS resilience, and autonomous systems, with intelligence focused on navigation attacks and ransomware; collaboration occurs through mode-specific Information Sharing and Analysis Centers (ISACs) and international coordination, while capabilities emphasize autonomous vehicle security and legacy fleet management.

Overall, Table 3 illustrates the necessity of customizing cybersecurity governance and operational strategies to sector-specific contexts, reinforcing that effective implementation depends on aligning governance priorities, intelligence focus, collaboration mechanisms, and capability development with the unique operational realities and threat landscapes of each critical infrastructure sector. This approach ensures that the strategic framework is not only theoretically robust but also practically applicable, enhancing resilience, risk management, and adaptive capacity across the United States' critical infrastructure systems.

Looking ahead, new challenges will test the adaptability of existing structures. Artificial intelligence presents both risks and opportunities (Brundage et al., 2018). Quantum computing threatens current encryption methods and calls for a shift to post-quantum cryptography (NIST, 2022). The globalization of supply chains increases reliance on components from potentially hostile countries. Additionally, climate change is increasingly linked to cybersecurity concerns, as infrastructure faces greater exposure to cyber-physical attacks. Successful implementation therefore requires aligning regulatory authority, operational responsibility, and long-term investment strategies across all levels of governance

Table 3: Sector-Specific Framework Customization Matrix

Sector	Governance Priorities	Intelligence Focus	Collaboration Needs	Capability Emphasis
Energy	OT-IT integration, supply chain, small operator support	State actor TTPs, supply chain threats	Interdependent utilities, fuel supply coordination	Legacy system security, workforce training
Financial	Fintechregulation, cross-border coordination	Fraud schemes, ransomware, APTs	International partnerships, vendor ecosystem	Quantum-safe cryptography, AI/ML security
Healthcare	Patient safety balance, device security, small facility support	Healthcare-targeting ransomware,medical device vulnerabilities	Hospital associations, device manufacturers	Backup/recovery, segmentation, security basics
Transportation	Modal coordination, GPS resilience, autonomous systems	Navigation attacks, ransomware, supply chain	Mode-specific ISACs, international coordination	Autonomous vehicle security, legacy fleet

3.4 International Comparison and Future Considerations

Global strategies provide useful insights into other governance frameworks. The European

Union's NIS2 Directive sets a mandatory cybersecurity standard, imposing significant fines for non-compliance (EU, 2022). The UK's National Cyber Security Centre emphasizes government-industry collaboration through active participation (NCSC, 2022). Australia's legislation also includes provisions for government assistance and intervention authorities (Australia, 2021). These international models illustrate how mandatory standards, enforcement mechanisms, and active government engagement can significantly elevate baseline cybersecurity performance.

Table 4 presents the **Framework Performance Measurement Dashboard**, which operationalizes the strategic cybersecurity framework by providing quantitative and qualitative metrics to evaluate governance effectiveness, resilience capabilities, collaboration quality, incident response efficiency, and investment efficiency across critical infrastructure sectors. The dashboard translates abstract framework principles into measurable indicators, enabling continuous monitoring, evidence-based decision-making, and accountability for both public and private stakeholders.

Governance effectiveness is assessed through metrics such as ISAC participation rates, policy update frequency, and compliance levels, providing insights into how well sector organizations adhere to strategic guidance and regulatory expectations. Resilience capabilities are measured by recovery time, backup integrity, and workforce readiness, reflecting an organization's ability to anticipate, absorb, adapt, and recover from cyber disruptions. Collaboration quality metrics, including information sharing volume and exercise participation, evaluate the efficiency and effectiveness of cross-sector and inter-organizational coordination, highlighting the degree to which interdependencies are managed proactively. Incident response is quantified via detection time, containment speed, and recovery duration, offering a performance-based perspective on operational readiness and crisis management. Investment efficiency considers security spending relative to returns on investment, ensuring that financial resources allocated to cybersecurity initiatives achieve tangible improvements in risk reduction and operational resilience.

By integrating these performance indicators, Table 4 provides a structured mechanism to assess the practical implementation of the strategic framework, enabling continuous improvement and adaptive learning. It ensures that sector-specific strategies are effectively aligned with overarching goals of enhancing resilience, strengthening governance, and maintaining operational continuity in the face of evolving cyber threats. This dashboard supports proactive decision-making and strategic prioritization, facilitating a measurable pathway toward national cybersecurity resilience.

Table 4: Framework Performance Measurement Dashboard

Metric Category	Key Indicators	Measurement Approach	Target Benchmarks
Governance Effectiveness	ISAC participation rates, policy update frequency, and compliance levels	Surveys, administrative data, audit results	85% sector participation, annual policy review, 95% compliance
Resilience Capabilities	Recovery time, backup integrity,workforce readiness	Exercise results, testing, certification tracking	RTO <24 hours for critical systems, quarterly tests passing

Collaboration Quality	Information sharing volume/velocity, exercise participation	System logs, event attendance, and feedback surveys	<1 hour for critical threat indicators, biannual exercises
Incident Response	Detection time, containment speed, recovery duration	Incident data analysis, postincident reviews	Detect <24 hours, contain <48 hours, recover <5 days
Investment Efficiency	Securityspendingratio, ROI calculations	Financial data, impact assessments	8-12% of IT budget, positive ROI on major initiatives

The proposed performance metrics enable continuous monitoring, support evidence-based decision-making, and provide accountability mechanisms for both public and private stakeholders. Looking ahead, new challenges will test the adaptability of existing structures. Artificial intelligence presents both risks and opportunities (Brundage et al., 2018; Amougou, 2023). Quantum computing threatens current encryption methods and calls for a shift to post-quantum cryptography (NIST, 2022). The globalization of supply chains increases reliance on components from potentially hostile countries. Additionally, climate change is increasingly linked to cybersecurity concerns, as infrastructure faces greater exposure to cyber-physical attacks (Okolo, 2023). Addressing these emerging challenges will require governance systems that are anticipatory rather than reactive, reinforcing the need for a strategic framework grounded in adaptability, collaboration, and resilience.

4.0 Conclusion

The current cybersecurity concerns of the United States' critical infrastructure necessitate a fundamentally different governance approach compared to the existing, fragmented compliance-based models. This paper presents a strategic framework designed to address this imperative, comprising four integrated pillars: adaptive governance structures capable of responding to threats in real time, the integration of threat intelligence to overcome information asymmetries, cross-sector collaboration mechanisms acknowledging infrastructure interdependence, and systematic resilience-building capabilities. The framework draws upon resilience theory, risk governance scholarship, and organizational learning, combining practical insights gained recently with international comparisons to ensure both theoretical rigor and operational feasibility. Achieving this requires long-term commitment from government entities and private sector stakeholders, appropriate resource allocation, the cultivation of trust through positive collaborative experiences, and a cultural shift recognizing cybersecurity as a strategic necessity. The path forward involves advancing beyond mere compliance to attain genuine resilience, transcending sectoral responses to develop comprehensive national strategies, and moving beyond reactive measures to proactive preparedness. This framework offers a strategic roadmap for such transformation; however, its success depends on a collective commitment to long-term resilience rather than short-term comfort and on investing in the capacity to withstand catastrophic events rather than merely responding to them. Further research is essential to evaluate the practical implementation of this framework, address technical challenges such as securing operational technologies and supply chains, and analyze the governance implications of emerging technologies transforming infrastructure. The stakes include national security, economic prosperity, and societal well-being, warranting nothing less than a dedicated effort to strengthen the

foundational governance structures upon which modern civilization relies.

5.0 References

American Hospital Association. (2023). Hospital Cyber Resiliency Initiative: Landscape Analysis. American Hospital Association. Retrieved from https://www.aha.org/guidesreports/2023-04-18-hospital-cyber-resiliency-initiative-landscape-analysis

Amougou, R. S. E. (2023). AI-Driven DevOps: Leveraging Machine Learning for Automated Software Delivery Pipelines. *Communication in Physical Sciences*, 9(4), 1010-1021.

Argyris, C., & Scho¨n, D. A. (1978). *Organizational learning: A theory of action perspective*. Addison-Wesley. ISBN 9780201001747

Akagbue, B. O., Aminu, M. A. B., Siame, T., Ofure, O. F., Amaobichukwu, C. T., Adinoyi, E. S., ... & Bolaji, O. (2023). Medical effect of emission from unregulated refineries at Rumuolumeni Community in Port Harcourt Rivers State Nigeria. Asian Journal of Medicine and Health, 21(12), 83-94. https://doi.org/10.9734/AJMAH/2023/v21i12963

Assante, M. J., & Lee, R. M. (2015). The industrial control system cyber kill chain. SANS Institute. Retrieved from https://www.sans.org/white-papers/36297

Australian Government. (2021). Security of Critical Infrastructure Act 2018 (compilation as of 2021). Retrieved from https://www.legislation.gov.au/Details/C2021C00246.

Aven, T., & Renn, O. (2010). Risk management and governance: Concepts, guidelines and applications. Springer. https://doi.org/10.1007/978-3-642-13926-0

Biden, J. R. (2021). Executive Order 14028: Improving the nation's cybersecurity. Federal Register, 86 FR 26633–26647. Retrieved from https://www.federalregister.gov/documents/2021/05/12/2021-09315/improving-the-nations-cybersecurity.

Brundage, M., et al. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. Future of Humanity Institute. https://doi.org/10.48550/arXiv.1802.07228.

Chowdhury, N., & Gkioulos, V. (2019). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, *34*, Article 100200. https://doi.org/10.1016/j.cosrev.2019.10200

Cybersecurity and Infrastructure Security Agency. (2021). *National Risk Management Center strategic plan 2021-2025*. Department of Homeland Security.
https://www.cisa.gov/resources-tools/resources/nrmc-strategic-plan

Cybersecurity and Infrastructure Security Agency. (2023). *People's Republic of China state-sponsored cyber actors living off the land to evade detection*. Alert AA23-144A. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a.

Cybersecurity and Infrastructure Security Agency. (2024). 2024 Critical Infrastructure Threat Assessment. Department of Homeland Security. Retrieved from https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience.

CMMI Product Team. (2010). *CMMI for development, version 1.3*. Carnegie Mellon Software Engineering Institute. https://doi.org/10.1184/R1/6572392.v1

Okolo, J. N. (2023). A Review of Machine and Deep Learning Approaches for Enhancing Cybersecurity and Privacy in the Internet of Devices. *Communication in Physical Sciences*. 9(4): 754-772.

Omosunlade, O. (2024). Curriculum Framework for Entrepreneurial Innovation among Special Needs Students in the Age of Artificial

Intelligence. *Communication in Physical Sciences*. 11(4): 1089- 1098.

U.S. Congress. (2015). Cybersecurity Information Sharing Act of 2015. Public Law 114-113, Division N. https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf.

U.S. Congress. (2018). Cybersecurity and Infrastructure Security Agency Act of 2018. Public Law 115-278. https://www.congress.gov/115/plaws/publ278/PLAW115publ278.pdf/

U.S. Congress. (2021). Infrastructure Investment and Jobs Act. Public Law 117-58. https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf.

Department of Homeland Security. (2022). Critical infrastructure sectors overview.https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/

Department of Homeland Security. (2023). *Cybersecurity workforce development*. https://www.dhs.gov/cybersecurity-workforce.

Environmental Protection Agency. (2022). Cybersecurity best practices for the water sector (EPA 817-B-22-001).https://www.epa.gov/waterresilience/cybersecurity-best-practices-water-sector.

European Union. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*, L333/80. https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA) 2023*. https://www.europol.europa.eu/publication-events/main-reports/iocta-2023.

Federal Bureau of Investigation. (2024). *Internet Crime Report 2023*. FBI Internet Crime Complaint Center. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf/

Financial Services Information Sharing and Analysis Center. (2023). FS-ISAC Annual Report 2023.https://www.fsisac.com/resources/2023-annual-report.

Gallagher, S. (2020). SolarWinds: How Russian spies hacked the Justice, State, Treasury, Energy, and Commerce Departments. Ars Technica.https://arstechnica.com/information-technology/2020/12/solarwinds-hack-explained.

Greenberg, A. (2019). Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. Doubleday. https://www.penguinrandomhouse.com/books/586697/sandworm-by-andy-greenberg/.

Hathaway, M., & Klimburg, A. (2023). Preliminary considerations: On national cyber security. In A. Klimburg (Ed.), *National cyber security framework manual* (pp. 1-22). NATO CCD COE. https://doi.org/10.1093/oso/9780190696726.003.0001.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75-105. https://doi.org/10.2307/25148625.

U.S. Department of Health and Human Services. (2013). *HIPAA Security Rule*. 45 CFR Part 164. https://www.hhs.gov/hipaa/for-professionals/security/index.html.

U.S. Department of Health and Human Services. (2024). *Breach portal: Notice to the Secretary of HHS breach of unsecured protected health information*. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, 4(1), 1-23. https://doi.org/10.1146/annurev.es.04.110173.000245.

International Electrotechnical Commission. (2018). *Security for industrial automation and control systems* (IEC 62443). https://webstore.iec.ch/publication/33615

International Organization for Standardization. (2013). *Information security management systems* (ISO/IEC 27001:2013). https://www.iso.org/standard/54534.html

Kaplan, R. S., & Norton, D. P. (1996). Using the balanced scorecard as a strategic management system. *Harvard Business Review*, *74*(1), 75–85.

Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., Lambert, J. H., Moon, A., & Thiel-Clemen, T. (2014). Changing the resilience paradigm. *Nature Climate Change*.

Linkov, I., & Palma-Oliveira, J. M. (Eds.). (2014). *Resilience and risk: Methods and application in environment, cyber and social domains*. Springer. https://doi.org/10.1007/978-94-017-8798-5.

Mandiant. (2023). *M-Trends 2023*. Google Cloud. https://www.mandiant.com/resources/reports/mtrends-2023.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, 15(4), 251-266. https://doi.org/10.1016/01679236(94)00041-2.

Moteff, J., & Parfomak, P. (2015). Critical infrastructure and key resources: Definition and identification (CRS Report RL32631). Congressional Research Service. https://sgp.fas.org/crs/homesec/RL32631.pdf.

North Atlantic Treaty Organization. (2023). Cyber defence. NATO. https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence.

UK National Cyber Security Centre. (2022). *Critical national infrastructure guidance*. https://www.ncsc.gov.uk/collection/cni-guidance.

North American Electric Reliability Corporation. (2023). *Critical infrastructure protection standards*. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Obama, B. (2013). *Presidential Policy Directive 21: Critical infrastructure security and resilience*. The White House. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resilience

Perlroth, N. (2021). *This is how they tell me the world ends: The cyberweapons arms race*. Bloomsbury Publishing.

Rahman, A. (2025). Circular economy approaches in chemical engineering: Redefining waste as resource. *Advances in Chemical Engineering*, *15*, Article 373. https://doi.org/10.35248/2090-4568.25.15.373

Renn, O., & Walker, K. D. (Eds.). (2008). *Global risk governance: Concept and practice using the IRGC framework*. Springer. https://doi.org/10.1007/978-1-4020-6799-0

Salatino, P., Chirone, R., & Clift, R. (2023). Chemical engineering and industrial ecology: Remanufacturing and recycling as process systems. *The Canadian Journal of Chemical Engineering*, *101*(1), 283–294. https://doi.org/10.1002/cjce.24625

Sanni, S. (2024). A review on machine learning and artificial intelligence in procurement: Building resilient supply chains for climate and economic priorities. *Communication in Physical Sciences*, *11*(4), 1099–1111.

Senge, P. M. (1990). *The fifth discipline: The art & practice of the learning organization*. Doubleday.

Siame, T., Abolade, Y. A., Omotayo, F., Nyarko, A. J., Aminu, M. B., Ogwurumba, U. A., Akagbue, B. O., Abdulmalik, F., & Zabidi, H. (2025). Potentially toxic elements in local cigarettes and marijuana leaves of Bauchi State, Nigeria: Public health and environmental implications. *Pollutants*, *5*(3), 26. https://doi.org/10.3390/pollutants5030026

Siame, T., Muzandu, K., Kataba, A., & M'Kandawire, E. (2023). Comparative determination of human health risks associated with consumption of groundwater contaminated with lead in selected areas surrounding the former lead mine in Kabwe and non-mining areas in Lusaka, Zambia. *International Journal of Community Medicine and Public Health*, *10*(11), 4089–4095. https://doi.org/10.18203/2394-6040.ijcmph20233434

Siame, T., Muzandu, K., Kataba, A., & Muzandu, J. (2024). A comparative assessment of Lead (Pb) concentration and physicochemical parameters in groundwater from the Kabwe mine and Lusaka non-mine sites, Zambia. *Discovery Environment*, *2*, Article 101. https://doi.org/10.1007/s44274-024-00132-3

Siame, T., Muzandu, K., Mulenga, K. K., & Dzombe, C. B. (2025). Lead-contaminated groundwater exposes residents to health risks in Makululu, Zambia. *Journal of Water and Health*, *23*(5), 615–629. https://doi.org/10.2166/wh.2025.343

Skierka, I., Morgus, R., Hohmann, M., & Maurer, T. (2015). *CSIRT basics for policy-makers: The history, types & culture of computer security incident response teams* (Policy Paper). Global Public Policy Institute & New America. https://gppi.net/assets/CSIRT_Basics_for_Policy-akers_May_2015_WEB.pdf

Slovic, P. (1987). Perception of risk. *Science*, *236*(4799), 280–285.https://doi.org/10.1126/science.3563507

Turton, W., & Mehrotra, K. (2021, June 4). Hackers breached Colonial Pipeline using compromised password. *Bloomberg*. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Wenger, E. (1998). *Communities of practice: Learning, meaning, and identity*. Cambridge University Press. https://doi.org/10.1017/CBO9780511803932

Yu, H., Zahidi, I., Fai, C. M., Liang, D., & Madsen, D. Ø. (2024). Mineral waste recycling, sustainable chemical engineering, and circular economy. *Results in Engineering*, *21*, Article 101865. https://doi.org/10.1016/j.rineng.2024.101865

Zetzsche, D. A., Buckley, R. P., Barberis, J. N., & Arner, D. W. (2017). Regulating a revolution: From regulatory sandboxes to smart regulation. *Fordham Journal of Corporate & Financial Law*, *23*(1), 31–103. https://doi.org/10.2139/ssrn.3018534

Declaration

Funding sources

No funding

Competing Financial Interests Statement:

There are no competing financial interests in this research work.

Ethical considerations

Not applicable

Data availability

The microcontroller source code and any other information can be obtained from the corresponding author via email.

Authors' Contribution

The author carried out the entire work, solely