Journal of Frontiers in Multidisciplinary Research

Next-Generation Business Intelligence Systems for Streamlining Decision Cycles in Government Health Infrastructure

Jeanette Uddoh [1], Daniel Ajiga [2*], Babawale Patrick Okare [3], Tope David Aduloju [4]
[1] Independent Researcher, Lagos Nigeria
[2] Independent Researcher, Mississippi, USA
[3] Infor-Tech Limited Aberdeen, UK
[4] Toju Africa, Nigeria

* Corresponding Author: **Daniel Ajiga**

Article Info

E-ISSN: 3050-9726
P-ISSN: 3050-9718
Volume: 02
Issue: 01
January-June 2021
Received: 06-05-2021
Accepted: 04-06-2021
Page No: 303-311

Abstract
In an increasingly digitized global landscape, public sector institutions have become critical nodes of national digital infrastructure, yet they remain highly vulnerable to cyber threats. As cyber-attacks grow in scale, complexity, and geopolitical significance, the urgency to establish robust and adaptive cyber risk models at the national level has intensified. This paper presents a comprehensive examination of the need for national cyber risk models specifically tailored to safeguard digital infrastructure within public sectors. It proposes a conceptual framework that integrates strategic, operational, and technological dimensions of cyber risk management and aligns them with the unique responsibilities and constraints of government agencies. The paper begins by contextualizing the vulnerability of public digital systems considering evolving cyber-attack patterns, such as ransomware, state-sponsored attacks, and critical infrastructure sabotage. Through a detailed literature review, it identifies the gaps in existing cyber risk models that primarily focus on corporate or defense-specific environments and do not fully address the public sector's multi-layered risk exposure. Drawing from theories in systems resilience, risk governance, and critical infrastructure protection, the study outlines a national cyber risk model that accommodates the institutional heterogeneity, policy fragmentation, and accountability demands typical of the public domain.
The model is based on a layered architecture: national strategic oversight, sectoral threat intelligence coordination, organizational vulnerability assessments, and real-time response protocols. Key dimensions include legal-regulatory compliance, cybersecurity culture, inter-agency data sharing, and adaptive incident response capabilities. The paper also includes case analyses from selected countries that have either successfully implemented national risk models or have faced significant breaches due to a lack of such frameworks. Implications for policy are explored in depth, especially in the context of cyber sovereignty, public trust, and international digital cooperation. Practical recommendations are provided for policymakers, security architects, and public IT managers on how to institutionalize cyber risk modeling within broader digital governance structures. Additionally, the paper identifies implementation challenges such as budgetary constraints, political inertia, legacy systems, and cyber skills gaps.By developing a holistic and scalable national cyber risk model, this study contributes to the academic and policy discourse on digital public safety. It aims to serve as a foundational resource for nations seeking to enhance their cyber resilience and protect public welfare in the face of ever-evolving digital threats.

DOI: https://doi.org/10.54660/.IJFMR.2021.2.1.303-311

Keywords: National Cyber Risk, Public Sector, Digital Infrastructure, Cyber Resilience, Risk Governance, Adaptive Response

1. Introduction

Digital transformation has revolutionized public sector operations, enabling efficiency, accessibility, and innovation in governance [1]. From digital identity systems to cloud-based tax platforms and national healthcare databases, governments increasingly rely on interconnected digital infrastructure to deliver essential services.

However, this dependency has concurrently exposed them to unprecedented levels of cyber vulnerability [2]. In recent years, there has been a surge in high-profile cyber incidents targeting public institutions examples include ransomware attacks on municipal governments, data breaches involving national ID systems, and state-sponsored intrusions into electoral infrastructure [3].

The threat landscape facing public sector digital infrastructure is distinct. Unlike private corporations, government entities are custodians of vast quantities of sensitive citizen data and critical infrastructure control systems [4]. They are also attractive targets for politically motivated cyber-attacks, cyber terrorism, and digital espionage. Furthermore, the public sector is often encumbered by bureaucratic inertia, outdated legacy systems, and limited cybersecurity expertise, making them uniquely exposed to sophisticated and persistent threats [5].

Despite this criticality, there is a marked lack of comprehensive, national-level cyber risk models designed with the public sector's unique characteristics in mind [6]. Existing cybersecurity frameworks often assume homogenous organizational structures and market-driven imperatives, which do not align well with public governance models, distributed authorities, and layered accountability mechanisms [7]. As a result, public institutions remain ill-equipped to proactively assess, quantify, and respond to systemic cyber risks.

This paper responds to this urgent gap by developing a National Cyber Risk Model tailored for public sector digital infrastructure [8]. It seeks to (i) define the unique risk landscape of public digital systems, (ii) identify structural and institutional vulnerabilities, (iii) review existing models and their limitations, and (iv) propose a contextually grounded framework that public sector institutions can adopt and adapt [9].

The model proposed in this paper is multidimensional, integrating governance, technological, human, and policy factors. It draws on the best international practices and cross-disciplinary research in cybersecurity, risk management, and digital public administration. This paper also aims to contribute to global policy discussions on cyber governance, with a particular focus on resilience-building, sovereignty, and cooperative threat intelligence [10].

In sum, the objective is to provide a roadmap that national governments and public IT administrators can utilize to build cyber-resilient systems that are not only secure but also transparent, adaptive, and citizen centric [11].

2. Literature Review

The literature on cyber risk modeling is vast but unevenly distributed across sectors. While substantial research has been conducted on enterprise cybersecurity and critical infrastructure protection in private industries, comparatively little attention has been given to the specific needs and vulnerabilities of public sector digital infrastructure [12]. This gap is especially significant given that public institutions are responsible for essential services, including healthcare, transportation, education, national identity, and internal security systems [13].

2.1 Cyber Risk Frameworks and Taxonomies

The foundational literature on cyber risk modeling often builds principles from the NIST Cybersecurity Framework, ISO/IEC 27001, and FAIR (Factor Analysis of Information Risk). These models provide structured approaches to identifying, assessing, and mitigating cyber risks in organizations [14]. However, most are developed with private enterprises in mind, where profit, shareholder value, and market dynamics dictate cybersecurity priorities [15]. Public sector organizations, on the other hand, must prioritize citizen welfare, democratic accountability, and regulatory compliance, which necessitates a different approach [16].

2.2 Public Sector Vulnerabilities

Research on cyber risk in the public sector points to specific weaknesses: aging legacy systems, fragmented IT governance, low cybersecurity maturity, and insufficient staff training [17]. Scholars such as Kshetri (2017) and Gill *et al*. (2019) highlight how bureaucratic constraints, slow procurement processes, and underinvestment in cybersecurity capabilities leave government institutions highly susceptible to attacks [18]. Moreover, public institutions are often targeted by adversaries with geopolitical motives an area explored extensively in studies on cyber warfare and national security [19].

2.3 Critical Infrastructure and Risk Governance

An adjacent field of study is critical infrastructure protection, particularly in the context of national security. Works by Dunn-Cavelty (2008) and Lewis (2010) provide frameworks for assessing cyber risk across energy grids, water supply systems, and transportation networks [20]. These studies underscore the importance of inter-agency coordination and public-private collaboration in safeguarding national systems. However, they still fall short of offering comprehensive models that integrate risk analysis, operational continuity, policy oversight, and adaptive resilience specific to broader public digital services [21].

2.4 Gaps in Existing Models

Most extant frameworks lack scalability across diverse government departments or fail to integrate non-technical factors such as public trust, institutional coordination, and political oversight. Additionally, they often treat cyber risk as static, failing to accommodate the fluid and adaptive nature of modern cyber threats [22]. Literature on resilience engineering and dynamic risk assessment, including Hollnagel (2011), is increasingly being recognized as critical to modern cyber risk approaches.

2.5 Contribution of This Study

This paper contributes to the literature by integrating insights from cybersecurity, public administration, risk science, and systems theory to propose a cyber risk model specifically suited for national application in the public sector. By doing so, it bridges the gap between theory and practice and provides a tool for building not just secure, but also agile and accountable digital public systems.

3. Theoretical Framework

The development of a national cyber risk model tailored to the public sector requires a multi-disciplinary theoretical foundation. The proposed model integrates concepts from three core theoretical pillars: risk governance theory, resilience systems theory, and public sector digital transformation frameworks. Together, these lenses offer a comprehensive understanding of the dynamics, constraints, and opportunities in securing national public digital

infrastructure [23].

3.1 Risk Governance Theory

At its core, cyber risk management involves processes of identification, evaluation, mitigation, and communication of risk. Risk governance theory, as articulated by the International Risk Governance Council (IRGC), goes beyond technical mitigation to encompass social, institutional, and political contexts [24]. It stresses the importance of stakeholder participation, transparency, and accountability in managing risks that are systemic and uncertain conditions that characterize cyber threats today.

This framework is particularly relevant for the public sector, where cyber risks affect not just organizational assets but public welfare, democratic processes, and national sovereignty. Risk governance emphasizes multi-level coordination, including inter-agency cooperation, public-private partnerships, and citizen engagement in building trust and resilience [25]. It also addresses normative dimensions—such as value judgments and political priorities which are integral to decisions about which digital assets to protect and how to allocate resources.

3.2 Resilience Systems Theory

Cyber resilience, as opposed to pure security, is increasingly recognized as a critical outcome for public digital systems. Resilience systems theory views organizations and infrastructures as adaptive systems capable of absorbing shocks, recovering, and even learning from disturbances. Hollnagel's four capacities of resilience responding, monitoring, learning, and anticipating form the backbone of this theoretical strand [26].

For public institutions, which often operate under rigid procedural and regulatory environments, embedding resilience requires systemic transformation. The theory supports a shift from reactive to proactive strategies, emphasizing redundancy, diversity, and continuous learning. These are essential to dealing with sophisticated and evolving cyber threats, including zero-day attacks, insider threats, and advanced persistent threats (APTs).

3.3 Digital Transformation in Public Administration

Digital transformation literature provides critical insights into how public institutions adopt and integrate technologies within bureaucratic structures. Theories such as the Technology-Organization-Environment (TOE) framework and New Public Management (NPM) reveal the organizational inertia, policy complexity, and cultural resistance that often hamper the modernization of public IT systems [27]. These dynamics must be factored into any realistic cyber risk model for government use.

Furthermore, digital transformation is not just about technology, it is also about organizational change, leadership, and capacity building. The theoretical integration of digital maturity models into cyber risk frameworks ensures that risk mitigation is aligned with the institution's technological readiness and governance maturity [28].

3.4 Integrative Framework

The resulting theoretical foundation supports the development of a layered, modular cyber risk model that reflects the complexity of public digital ecosystems. It allows for both strategic (national policy, inter-sectoral coordination) and operational (technical assessments, staff training, response planning) components, ensuring that the model is both scalable and adaptable [29].

This integrated framework enables the design of a cyber risk model that is not only technically sound but also politically viable and administratively actionable critical requirements for public sector implementation [30].

4. Methodology

The methodology underpinning this study is grounded in a qualitative, interdisciplinary approach designed to synthesize theoretical concepts, empirical insights, and policy practices into a practical national cyber risk framework for the public sector. The approach is exploratory and conceptual in nature, aimed at generating a model that is contextually relevant, scalable, and adaptable to various levels of government and administrative structures.

4.1 Research Design

This paper employs a conceptual modeling methodology, which draws upon comparative case analysis, critical synthesis of secondary data, and theoretical triangulation. Unlike empirical research that tests hypotheses, conceptual modeling aims to develop new frameworks by integrating diverse sources of evidence and theoretical constructs. This approach is particularly suited for addressing complex, systemic challenges such as national cyber risk governance where variables are interdependent, outcomes are uncertain, and standardized models are lacking.

4.2 Data Sources

Three categories of secondary data were analyzed:

1. Academic Literature: A comprehensive review was conducted of peer-reviewed journals in cybersecurity, public administration, information systems, risk management, and resilience engineering. This helped identify existing models, theoretical gaps, and best practices [31].
2. Policy and Regulatory Documents: Cybersecurity strategies, white papers, and legal frameworks from key national cybersecurity agencies (e.g., U.S. Cybersecurity and Infrastructure Security Agency, UK National Cyber Security Centre, EU ENISA) were examined to understand how governments currently frame and implement cyber risk governance [32].
3. Case Studies and Incident Reports: Publicly available data from documented cyber-attacks on public institutions such as the WannaCry attack on the UK NHS, the SolarWinds breach in the U.S., and ransomware attacks on South African municipalities were analyzed to understand real-world vulnerabilities, response patterns, and policy implications [33].

4.3 Analytical Strategy

The analytical process followed three stages:

- Thematic Coding: Key themes were identified from the literature and policy documents, including risk governance, incident response, public-sector IT readiness, inter-agency coordination, and institutional resilience [34].
- Comparative Synthesis: Cyber risk approaches were compared across countries and agencies to extract common elements and highlight divergent strategies. Attention was given to contextual factors such as political structure, digital maturity, and administrative

culture.
- Framework Development: Based on the synthesis, a layered cyber risk model was constructed. This model was iteratively refined to integrate technical, organizational, and governance dimensions while maintaining flexibility for different institutional settings.

4.4 Limitations
While this methodology allows for a robust conceptual foundation, it does not offer empirical validation of the model's implementation or outcomes. Future research should consider mixed-methods evaluations, simulations, or field-testing in collaboration with public sector institutions.

5. Proposed Cyber Risk Model for the Public Sector
The cyber threat landscape facing public sector institutions demands a comprehensive, scalable, and adaptive framework for identifying, assessing, and managing digital risks at the national level. Drawing on the insights from the preceding theoretical and methodological sections, this paper proposes a Layered National Cyber Risk Model (LNCRM) designed specifically for public digital infrastructure. The model comprises five interdependent layers: National Strategy and Governance, Sectoral Coordination, Organizational Resilience, Technical Risk Management, and Public Engagement & Transparency [35].

5.1 Layer 1: National Strategy and Governance
At the apex of the model is the strategic oversight function provided by a national cybersecurity governance body typically a centralized agency operating under the executive branch. This body is responsible for:
- Defining national cybersecurity priorities.
- Coordinating cross-sectoral policies.
- Establishing minimum security standards for public IT systems.
- Managing international cooperation and cyber diplomacy.

This strategic layer also includes legal frameworks, budg*et al*locations, and regulatory mandates that empower public institutions to act decisively against cyber threats. Importantly, it fosters a whole-of-government approach to cyber resilience, moving beyond siloed agency-level initiatives [36].

5.2 Layer 2: Sectoral Coordination
This layer recognizes that ministries and agencies in health, finance, education, transportation, and other sectors face distinct threats and operate under varying levels of digital maturity. Therefore, the model includes sector-specific cybersecurity units that function under the umbrella of national governance but tailor strategies to their operational realities.
Key functions include:
- Threat intelligence sharing.
- Sector-based vulnerability assessments.
- Development of industry-specific cybersecurity protocols.
- Training programs aligned to sector-specific use cases.

5.3 Layer 3: Organizational Resilience
Each public agency must have an internal cyber risk management unit responsible for:
- Conducting regular risk assessments and audits.
- Maintaining business continuity and incident response plans.
- Ensuring cybersecurity is embedded in procurement, project design, and daily operations.

This layer emphasizes resilience capacity-building, such as enhancing human capital, establishing rapid response teams, and improving digital literacy among staff. Integration with legacy systems and the use of Zero Trust Architecture principles are also encouraged here [35].

5.4 Layer 4: Technical Risk Management
This layer encompasses the operational and technical dimensions of cybersecurity, including:
- Continuous network monitoring.
- Endpoint security.
- Identity and access management.
- Penetration testing.
- Incident detection and mitigation.

Advanced technologies such as artificial intelligence for threat detection, blockchain for secure records, and encryption standards for data privacy are also integrated here [37]. Importantly, this layer supports interoperability across government platforms while enforcing centralized security protocols.

5.5 Layer 5: Public Engagement and Transparency
Public trust is a cornerstone of successful digital governance. This layer incorporates mechanisms to ensure citizen awareness, transparency, and accountability, including:
- Cyber hygiene campaigns for citizens.
- Public disclosure protocols for data breaches.
- Mechanisms for citizen feedback and digital grievance redressal.
- Open reporting on cybersecurity performance indicators.

By involving citizens as stakeholders in cyber resilience, the model fosters a culture of shared responsibility and digital citizenship [38].
In summary, the LNCRM provides a structured, multi-layered approach to national cyber risk governance tailored to the complex operational realities of the public sector. It enables vertical coordination (from national to organizational levels) and horizontal integration (across agencies and sectors), ensuring that cyber risk management is both systemic and sustainable.

6. Comparative Case Studies
To illustrate the applicability and effectiveness of the Layered National Cyber Risk Model (LNCRM**)**, this section presents case studies of countries that have made significant strides in strengthening cyber resilience within their public sector digital infrastructures. These case studies highlight the unique challenges, strategies, and successes of different national contexts, offering valuable lessons for the implementation of the proposed model [39].

6.1 Case Study 1: Estonia’s National Cybersecurity Framework
Estonia is often considered a global leader in public sector digital transformation and cybersecurity. The country’s experience provides a valuable example of how a well-

coordinated national strategy can improve cyber resilience. Estonia's Cybersecurity Strategy involves a combination of central government oversight (managed by the Estonian Information System Authority) and sectoral coordination through sectoral cybersecurity councils [40]. These councils ensure that individual ministries, from health to finance, implement cybersecurity measures tailored to their specific needs while aligning national priorities.

Key Features:

- National Strategy: Estonia's national strategy includes mandatory cybersecurity requirements for public services and critical infrastructure. The country also established a robust e-government system that integrates security by design into all digital services.
- Public Engagement: Estonia's approach to public engagement is another hallmark. Citizens are encouraged to participate in digital governance through the e-Estonia initiative, which promotes digital literacy and transparency, ensuring that the public remains informed and engaged in the cybersecurity discourse.

The Estonian example demonstrates the effectiveness of having a strong, central governance body, coupled with sectoral coordination, to ensure comprehensive coverage and an adaptive response to evolving cyber threats.

6.2 Case Study 2: United States – CISA and Critical Infrastructure Protection

In the United States, the Cybersecurity and Infrastructure Security Agency (CISA), part of the Department of Homeland Security, plays a key role in protecting critical infrastructure, including public sector systems, from cyber threats. The U.S. model provides an example of a national body that integrates cybersecurity efforts across multiple sectors, particularly in the context of public sector digital infrastructure.

Key Features:

- Sectoral Coordination: CISA works closely with both public agencies and private-sector entities to develop tailored cybersecurity frameworks for sectors such as healthcare, energy, and transportation. The National Infrastructure Protection Plan (NIPP) emphasizes sector-specific risk management strategies [41].
- National Risk Register: CISA's National Risk Register identifies the most critical cyber risks facing the country and is used as a guide for cybersecurity policies across federal, state, and local governments.

This model emphasizes strong federal oversight and coordination y*et al*so highlights the need for sector-specific strategies and collaboration with industry stakeholders to ensure that vulnerabilities across different sectors are adequately addressed.

6.3 Case Study 3: Singapore – National Cybersecurity Strategy

Singapore's approach to cybersecurity combines both strategic oversight and detailed operational measures at the national level, enabling it to develop a robust and resilient cybersecurity posture for the public sector. The country's Cybersecurity Agency of Singapore (CSA) is responsible for overseeing the implementation of the Singapore Cybersecurity Strategy, which aims to enhance national resilience against cyber threats [42].

Key Features

- National Cybersecurity Governance: Singapore's Cybersecurity Strategy emphasizes whole-of-nation involvement in cybersecurity, with government agencies, the private sector, and citizens all playing active roles. The CSA sets the framework for cybersecurity initiatives and coordinates national cyber resilience efforts.
- Resilience Engineering: In addition to risk prevention, Singapore's strategy places a strong focus on cyber resilience, ensuring that public sector systems are not only protected from attacks but can also recover quickly in the event of a breach. This includes incident response planning, system redundancies, and business continuity measures.

Singapore's model highlights the importance of resilience engineering, where cybersecurity is viewed not just as protection but as a dynamic and ongoing process of adaptation to new risks.

6.4 Lessons Learned and Implications for the LNCRM

The comparative analysis of these case studies offers several key lessons for the development and implementation of the Layered National Cyber Risk Model:

1. Centralized Governance with Sectoral Flexibility: A strong national governance body is essential, but sectoral coordination should ensure that tailored strategies are implemented based on the unique needs of different public sector departments.
2. Collaboration with Stakeholders: Public-private partnerships and international cooperation are integral to achieving comprehensive cybersecurity protection.
3. Focus on Resilience: Cybersecurity efforts must include not only risk mitigation but also planning for recovery and continuity, ensuring that public services remain operational even after cyber incidents.

The cases also underscore the importance of integrating public engagement and transparency into cybersecurity strategies [43]. By promoting digital literacy and public awareness, governments can enhance the resilience of their digital infrastructures and foster a culture of shared responsibility in cybersecurity.

7. Policy Implications and Recommendations

The development of a **Layered National Cyber Risk Model (LNCRM)** for public sector digital infrastructure offers several policy implications that can inform the evolution of national cybersecurity strategies. Drawing from the comparative case studies and the proposed model, this section highlights key recommendations for policymakers, government agencies, and public institutions looking to enhance their cyber resilience and safeguard digital infrastructures in an increasingly interconnected world.

7.1 Strengthening National Cybersecurity Governance

A central pillar of the LNCRM is the importance of national cybersecurity governance. Considering growing digital threats, countries must prioritize the creation or enhancement of national agencies tasked with overseeing cybersecurity across all sectors. Governments should establish or strengthen centralized cybersecurity bodies with clear mandates to coordinate the actions of various public sector

institutions [44]. These agencies should possess sufficient authority to enforce compliance with cybersecurity standards, monitor emerging threats, and ensure that cybersecurity is integrated into all aspects of public sector operations.

Additionally, inter-agency collaboration is essential for ensuring that cybersecurity practices are harmonized and aligned across sectors. Policymakers must promote whole-of-government approaches that bring together ministries, regulatory bodies, and other key stakeholders to develop and implement cohesive cybersecurity policies and frameworks.

7.2 Promoting Sectoral Coordination

While national governance is important, the success of any cybersecurity strategy depends on effective sectoral coordination. Policymakers should invest in creating sector-specific cybersecurity units that are aligned with the national framework but are empowered to develop tailored strategies for their specific sector needs. These units should be responsible for conducting threat assessments, defining specific risk management protocols, and ensuring that the sector's digital infrastructure is secure and resilient.

Cross-sector collaboration must also be encouraged. For example, critical sectors such as healthcare, energy, and transportation often share common infrastructure and face similar cyber risks. Governments should facilitate sectoral working groups to foster information-sharing and collective problem-solving, thus ensuring that cyber risk management efforts are coordinated, rather than fragmented.

7.3 Fostering Public-Private Partnerships

The growing complexity of cyber threats requires collaborative efforts between the public and private sectors. Governments must develop public-private partnership (PPP) models that encourage the sharing of cyber threat intelligence, best practices, and incident reports. This can be achieved through the establishment of formal cybersecurity information-sharing platforms, where public agencies and private companies can exchange insights into vulnerabilities and emerging risks [45].

Public institutions must also collaborate with the private sector to develop cybersecurity tools and technologies suited to the unique needs of the public sector. In some cases, public agencies may require tailored cybersecurity technologies, such as secure cloud solutions or advanced threat detection systems, which may not be available from generic vendors. By working with private industry, governments can ensure that the tools and technologies deployed are fit for purpose and resilient to new cyber risks.

7.4 Building Organizational Resilience

Beyond governance and coordination, organizational resilience is a critical component of cybersecurity strategy. Policymakers should encourage the development of organizational resilience plans across all public institutions, focusing on aspects such as incident response, business continuity, and employee training [46].

Government agencies must be encouraged to adopt comprehensive incident response plans that ensure a timely and effective response to cyber incidents, minimizing downtime and ensuring public services remain operational. Resilience should also be built into organizational culture, with cybersecurity awareness training offered regularly to employees at all levels. This will enhance the human element of security, ensuring that personnel can recognize potential threats and take appropriate action.

Moreover, public agencies should integrate business continuity planning and disaster recovery strategies into their daily operations, ensuring that systems can recover quickly after a cyberattack. This includes ensuring that critical digital infrastructures have redundancy mechanisms in place and that key systems can be restored in a controlled manner after a disruption.

7.5 Enhancing Public Engagement and Transparency

Governments must ensure that public engagement is a core component of national cybersecurity strategies. Transparency, accountability, and public awareness are vital in building trust and ensuring that citizens understand their role in securing digital spaces. Policymakers should promote cyber hygiene campaigns to educate the public on best practices for securing personal devices, protecting sensitive information, and responding to cyber threats.

Additionally, public reporting of cyber incidents should be mandated. When cyberattacks occur, government agencies should provide clear, transparent updates to citizens, ensuring that they understand the nature of the attack, the actions taken to address it, and any potential consequences. This kind of transparency not only builds trust but also empowers citizens to be more vigilant and proactive in safeguarding their own digital infrastructure [46].

7.6 Conclusion

The recommendations outlined above reflect the need for a comprehensive, layered approach to managing cyber risk within public sector institutions. By prioritizing strong national governance, fostering sectoral coordination, encouraging public-private partnerships, building organizational resilience, and enhancing public engagement, governments can significantly strengthen the cybersecurity posture of their public digital infrastructures.

The proposed Layered National Cyber Risk Model (LNCRM) provides a flexible framework that can be tailored to the specific needs of different countries, enabling them to build adaptive, resilient cybersecurity strategies. Policymakers must act swiftly and decisively to implement these measures to ensure the continued protection and integrity of public sector digital infrastructures in an increasingly interconnected and digitally dependent world.

8. Conclusion

The increasing complexity of cyber threats and the growing reliance on digital infrastructure by public sector institutions underscore the critical need for a comprehensive and adaptive national cybersecurity framework. The Layered National Cyber Risk Model (LNCRM) proposed in this paper offers a structured approach for safeguarding public digital infrastructures by emphasizing the integration of national governance, sectoral coordination, organizational resilience, technical risk management, and public engagement. This multi-layered approach is designed to be scalable, adaptable, and responsive to the evolving cyber threat landscape faced by public sector organizations.

8.1 The Need for a Holistic Cybersecurity Strategy

The rapid digitalization of government services, the rise of interconnected public infrastructure, and the growing sophistication of cyberattacks have made cybersecurity a top

priority for governments worldwide. However, many public sector institutions still lack the necessary frameworks to assess, manage, and mitigate cyber risks effectively. The absence of comprehensive, layered cybersecurity strategies leaves public institutions vulnerable to attacks that could undermine critical services, disrupt operations, and damage public trust.

The LNCRM provides a comprehensive model that goes beyond traditional risk management approaches. By incorporating governance, coordination, resilience, and public engagement, the model ensures that national cybersecurity strategies are robust, coordinated, and capable of adapting to new and emerging threats. The model also highlights the importance of integrating both technical and non-technical measures, ensuring that cybersecurity is not only about protecting systems and data but also about creating resilient institutions and promoting informed public participation in securing the digital environment.

8.2 Key Findings and Contributions

The research underscores the importance of national leadership in cybersecurity governance. Countries that have developed robust cybersecurity frameworks, such as Estonia, the United States, and Singapore, provide valuable insights into the key components of effective national cyber risk management. These case studies demonstrate that central governance bodies, combined with sectoral coordination, organizational resilience, and public-private partnerships, are essential for creating a unified and resilient cybersecurity strategy.

Moreover, the paper emphasizes that cyber resilience is not just about preventing cyberattacks but also about preparing for and responding to them effectively. This holistic approach ensures that public institutions can recover quickly from cyber incidents, minimizing disruption to essential services and protecting citizens' trust in government operations.

One of the key contributions of this paper is its focus on public engagement as a critical aspect of national cybersecurity strategies. Many countries have traditionally treated cybersecurity as an isolated concern managed by technical experts and government agencies. However, public engagement and transparency are necessary to build a culture of cybersecurity, where citizens understand their role in protecting both their own data and national digital infrastructure. The LNCRM proposes actionable strategies for involving citizens in national cybersecurity efforts through educational campaigns, open reporting, and transparency in incident management.

8.3 Policy Implications and Future Research

The policy recommendations presented in this paper offer actionable strategies for governments to strengthen their cybersecurity governance [47]. By focusing on centralized oversight, sector-specific coordination, public-private partnerships, organizational resilience, and public engagement, governments can create a robust cybersecurity framework that addresses both technical and human aspects of risk management [48].

However, this research also highlights the need for further empirical studies to test the effectiveness of the LNCRM in practice. Future research could explore the implementation of the model in different national contexts, analyzing the challenges and benefits of adopting a layered approach to cybersecurity [49]. Additionally, future studies should consider the role of emerging technologies, such as artificial intelligence, machine learning, and blockchain, in enhancing the cybersecurity resilience of public sector infrastructures [50].

9. Conclusion

In conclusion, the Layered National Cyber Risk Model (LNCRM) offers a valuable conceptual framework for addressing the growing threats to public sector digital infrastructures. The model's focus on multi-layered governance, sectoral coordination, organizational resilience, and public engagement provides a comprehensive approach to managing cyber risk in the public sector. Governments must act swiftly to implement these strategies to safeguard critical infrastructure, protect sensitive data, and maintain the trust of citizens in the digital age. As cyber threats continue to evolve, the need for adaptive and resilient cybersecurity strategies has never been more urgent.

The model presented in this paper contributes to the growing body of knowledge on cybersecurity risk management, offering both theoretical insights and practical guidance for policymakers, public institutions, and researchers looking to improve national cyber resilience. Through continued research, collaboration, and innovation, the public sector can build a secure digital environment that fosters trust, ensures continuity, and enhances the overall well-being of citizens in an increasingly interconnected world.

10. References

1. Sarker MNI, Wu M, Hossin MA. Smart governance through bigdata: Digital transformation of public agencies. In: 2018 International Conference on Artificial Intelligence and Big Data (ICAIBD); May 2018. p. 62-70. doi:10.1109/ICAIBD.2018.8396168.
2. Kuldosheva G. Challenges and opportunities of digital transformation in the public sector in transition economies: Examination of the case of Uzbekistan. ADBI Working Paper Series. 2021;Working Paper 1248. Available from: https://www.econstor.eu/handle/10419/238605
3. Adema D, Blenkhorn S, Houseman S. Scaling-up Impact: Knowledge-based Organizations Working Toward Sustainability.
4. West DM. Digital Government: Technology and Public Sector Performance. Princeton University Press; 2005.
5. Ajiga DI. Strategic Framework for Leveraging Artificial Intelligence to Improve Financial Reporting Accuracy and Restore Public Trust. Int J Multidiscip Res Growth Eval. 2021;2(1):882-892. doi:10.54660/.IJMRGE.2021.2.1.882-892.
6. Ndou VD. E – Government for Developing Countries: Opportunities and Challenges. Electron J Inf Syst Dev Ctries. 2004 Jun;18(1):1-24. doi:10.1002/j.1681-4835.2004.tb00117.x.
7. Strategic Management Competencies for Radical Innovation in a Volatile, Uncertain, Complex, and Ambiguous (VUCA) World: a Systematic Review of the Evidence - ProQuest [Internet]. Available from: https://www.proquest.com/openview/bbca5033480751da492c3634896f4fa8/1?cbl=18750&diss=y&pq-origsite=gscholar
8. Dhillon R, Nguyen QC, Kleppestø S, Hellström M. Strategies to Respond to a VUCA World.
9. Mergel I, Edelmann N, Haug N. Defining digital

transformation: Results from expert interviews. Gov Inf Q. 2019 Oct;36(4):101385. doi:10.1016/j.giq.2019.06.002.
10. The Experience of Strategic Thinking in a Volatile, Uncertain, Complex, and Ambiguous (VUCA) Environment - ProQuest [Internet]. Available from: https://www.proquest.com/openview/c1a7221132765c5fab6d96b8098d0f2e/1.pdf?cbl=18750&diss=y&pq-origsite=gscholar
11. Habibi S. The Role of Smart Technologies in the Relationship Between Volatile, Uncertain, Complex and Ambiguous Business Environment (VUCA) and Organizational Agility: Industrial Enterprises Research.
12. Kaivo-oja JRL, Lauraeus IT. The VUCA approach as a solution concept to corporate foresight challenges and global technological disruption. Foresight. 2018 Mar;20(1):27-49. doi:10.1108/FS-06-2017-0022.
13. Thriving, Not Just Surviving in Changing Times: How Sustainability, Agility and Digitalization Intertwine with Organizational Resilience [Internet]. Available from: https://www.mdpi.com/2071-1050/13/4/2052
14. Bhattacharjee A, *et al*. Toward Rapid Development and Deployment of Machine Learning Pipelines across Cloud-Edge. In: Deep Learning for Internet of Things Infrastructure. CRC Press; 2021.
15. Dunleavy P, Margetts H, Bastow S, Tinkler J. New Public Management Is Dead—Long Live Digital-Era Governance. J Public Adm Res Theory. 2006 Jul;16(3):467-494. doi:10.1093/jopart/mui057.
16. Dawes SS. The Evolution and Continuing Challenges of E-Governance. Public Adm Rev. 2008;68(s1):S86-S102. doi:10.1111/j.1540-6210.2008.00981.x.
17. Falk S, Römmele A, Silverman M. The Promise of Digital Government. In: Digital Government: Leveraging Innovation to Improve Public Sector Performance and Outcomes for Citizens. Cham: Springer International Publishing; 2017. p. 3-23. doi:10.1007/978-3-319-38795-6_1.
18. Financing Climate-Smart Agriculture: a case study from the Indo-Gangetic Plains | Mitigation and Adaptation Strategies for Global Change [Internet]. Available from: https://link.springer.com/article/10.1007/s11027-024-10127-3
19. Mahmudnia D, Arashpour M, Yang R. Blockchain in construction management: Applications, advantages and limitations. Autom Constr. 2022 Aug;140:104379. doi:10.1016/j.autcon.2022.104379.
20. Lee JW. Big Data Strategies for Government, Society and Policy-Making. J Asian Finance Econ Bus. 2020;7(7):475-487. doi:10.13106/jafeb.2020.vol7.no7.475.
21. Soonawalla T. Critical infrastructure protection in Canada: focus on the energy sector. 2009. Available from: http://hdl.handle.net/1880/104168
22. Fang Z. E-Government in Digital Era: Concept, Practice, and Development. 2002;10.
23. Agarwal S, *et al*. Unleashing the power of disruptive and emerging technologies amid COVID-19: A detailed review. arXiv. 2021 Apr 19. doi:10.48550/arXiv.2005.11507
24. Gölgeci I, Arslan A, Dikova D, Gligor DM. Resilient agility in volatile economies: institutional and organizational antecedents. J Organ Change Manag. 2019 Nov;33(1):100-113. doi:10.1108/JOCM-02-2019-0033.
25. A Conceptual Framework for AI-Driven Digital Transformation: Leveraging NLP and Machine Learning for Enhanced Data Flow in Retail Operations [Internet]. ResearchGate. Available from: https://www.researchgate.net/publication/390928712_A_Conceptual_Framework_for_AI-Driven_Digital_Transformation_Leveraging_NLP_and_Machine_Learning_for_Enhanced_Data_Flow_in_Retail_Operations
26. Navigating the Human Side of Workplace Conflict: A Comparative Study of Organizational Ombuds' Similarities and Differences - ProQuest [Internet]. Available from: https://www.proquest.com/openview/d8d591aee6f77dd684ddb9e4a0084f41/1.pdf?cbl=18750&diss=y&pq-origsite=gscholar
27. Mushtaq S. Modern Cyber-Attacks and Cloud Security: Strengthening Information Security in Emerging Technologies.
28. Doyle KM, Ed M. MAPPING THE LANGUAGE OF SCIENCE AND SCIENCE TEACHING PRACTICES: A CASE STUDY OF EARLY CHILDHOOD SCHOOL SCIENCE.
29. Huxham C, Vangen S. LEADERSHIP IN THE SHAPING AND IMPLEMENTATION OF COLLABORATION AGENDAS: HOW THINGS HAPPEN IN A (NOT QUITE) JOINED-UP WORLD.
30. Leader Readiness in a Volatile, Uncertain, Complex, and Ambiguous (VUCA) Business Environment - ProQuest [Internet]. Available from: https://www.proquest.com/openview/442e280943a3d94776d6f8d06e825a37/1?cbl=18750&diss=y&pq-origsite=gscholar
31. Internet of Things and Distributed Denial of Service as Risk Factors in Information Security | IntechOpen [Internet]. Available from: https://www.intechopen.com/chapters/73910
32. Eld H, Johansson E. Innovation Strategies in a VUCA World.
33. Elumilade OO, Ogundeji IA, Achumie GO, Omokhoa HE, Omowole BM. Enhancing fraud detection and forensic auditing through data-driven techniques for financial integrity and security. J Adv Educ Sci. 2021 Dec;1(2).
34. Zaslavska K, Zaslavska Y. Impact of global factors on entrepreneurial structures: navigating strategic adaptation and transformation amidst uncertainty. Actual Probl Innov Econ Law. 2024 Sep;2024(5):26-32. doi:10.36887/2524-0455-2024-5-5.
35. Akinade AO, Adepoju PA, Ige AB, Afolabi AI, Amoo OO. A conceptual model for network security automation: Leveraging ai-driven frameworks to enhance multi-vendor infrastructure resilience. Int J Sci Technol Res Arch. 2021 Sep;1(1):39-59. doi:10.53771/ijstra.2021.1.1.0034.
36. 39675076.pdf [Internet]. Available from: https://core.ac.uk/download/pdf/39675076.pdf
37. Kamaldeen O. A Systemic Approach to Strategic Planning: Navigating Complexity with Clarity.
38. Spayd MK, Madore M. Agile Transformation: Using the Integral Agile Transformation FrameworkTM to Think and Lead Differently. Addison-Wesley Professional; 2020.

39. Olson EM, Olson KM, Czaplewski AJ, Key TM. Business strategy and the management of digital marketing. Bus Horiz. 2021 Mar;64(2):285-293. doi:10.1016/j.bushor.2020.12.004.
40. Larson RC. Commentary—Smart Service Systems: Bridging the Silos. Serv Sci. 2016 Dec;8(4):359-367. doi:10.1287/serv.2016.0140.
41. Disrupted Leadership: Strategies and Practices of Leaders in a VUCA World - ProQuest [Internet]. Available from: https://www.proquest.com/openview/fa2e11e70a41dbb211b963aab37b2f3f/1?cbl=18750&diss=y&pq-origsite=gscholar
42. Ogunsola KO, Balogun ED. Enhancing Financial Integrity Through an Advanced Internal Audit Risk Assessment and Governance Model. Int J Multidiscip Res Growth Eval. 2021;2(1):781-790. doi:10.54660/.IJMRGE.2021.2.1.781-790.
43. [Internet]. Available from: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=b36c0aa2777430eda7c3966174e3ed548fd4194f
44. Adekunle BI, Chukwuma-Eke EC, Balogun ED, Ogunsola KO. A Predictive Modeling Approach to Optimizing Business Operations: A Case Study on Reducing Operational Inefficiencies through Machine Learning. Int J Multidiscip Res Growth Eval. 2021;2(1):791-799. doi:10.54660/.IJMRGE.2021.2.1.791-799.
45. Teece D, Peteraf M, Leih S. Dynamic Capabilities and Organizational Agility: Risk, Uncertainty, and Strategy in the Innovation Economy. Calif Manage Rev. 2016 Aug;58(4):13-35. doi:10.1525/cmr.2016.58.4.13.
46. Ogunsola KO, Balogun ED. Enhancing Financial Integrity Through an Advanced Internal Audit Risk Assessment and Governance Model. Int J Multidiscip Res Growth Eval. 2021;2(1):781-790. doi:10.54660/.IJMRGE.2021.2.1.781-790.
47. Srinivas J, Das AK, Kumar N. Government regulations in cyber security: Framework, standards and recommendations. Future Gener Comput Syst. 2019 Mar;92:178-188. doi:10.1016/j.future.2018.09.063.
48. Dean B, McDermott R. A Research Agenda to Improve Decision Making in Cyber Security Policy. Penn State J Law Int Aff. 2017;5:29.
49. Tasheva I. Cybersecurity post-COVID-19: Lessons learned and policy recommendations. Eur View. 2021 Oct;20(2):140-149. doi:10.1177/17816858211059250.=
50. National Cyber Governance Awareness Policy and Framework | International Journal of Legal Information | Cambridge Core [Internet]. Available from: https://www.cambridge.org/core/journals/international-journal-of-legal-information/article/abs/national-cyber-governance-awareness-policy-and-framework/0DE344E28ACC8DC7D1DFCD7D07841E46