National Cyber Resilience Index: A Data-Driven Framework for Measuring Preparedness

Ogochukwu Susan Ndibe

University of Central Missouri

Cybersecurity and Information Assurance

https://orcid.org/0009-0004-1133-7036

Abstract

This paper presents a data-driven framework for developing a National Cyber Resilience Index (NCRI) a composite, quantitative tool to assess a nation's ability to prepare for, absorb, recover from, and adapt to cyber incidents. Unlike conventional cybersecurity maturity models, the proposed NCRI integrates heterogeneous data sources, advanced graph-based analytics, and adaptive metrics to capture the dynamic nature of national cyber preparedness. The framework encompasses four core dimensions Governance, Technical Capabilities, Human Capital, and Collaboration supported by measurable indicators and validated using cross-index benchmarking and statistical analysis. Through a mixed-methods approach combining systematic review, data modeling, and expert validation, the NCRI enables comparative resilience assessment and policy optimization. The study concludes with implications for policymakers, industry, and researchers, emphasizing ethical AI use, quantum-safe encryption, and standardized resilience metrics for future work.

Keywords: cyber resilience, data analytics, national security, graph neural networks, resilience index, ETL, explainable AI

1 Introduction

1.1 Context and Significance of Cyber Resilience Measurement

The escalating frequency and sophistication of cyber threats pose substantial risks to national security, economic stability, and critical infrastructure worldwide. Traditional cybersecurity approaches, primarily focused on prevention, prove insufficient given the inevitability of security breaches [1]. A more comprehensive paradigm, cyber resilience, has emerged, emphasizing an entity's capacity to prepare for, absorb, recover from, and adapt to adverse cyber events while maintaining essential functions [1]. This conceptual shift moves beyond mere protection, acknowledging that incidents will occur and focusing on sustained operational continuity. Measuring cyber resilience at a national level presents a unique challenge, necessitating a holistic view that integrates diverse data points from various sectors. Such measurement is crucial for identifying vulnerabilities, assessing preparedness, and guiding strategic investments in national cyber defense

capabilities [2]. Without robust, data-driven metrics, policymakers struggle to evaluate the effectiveness of existing cyber strategies or prioritize resources for maximum impact [3]. The absence of a standardized, comprehensive framework hinders comparative analysis across nations and limits the ability to learn from best practices [4]. A national cyber resilience index offers a quantitative tool for understanding a country's posture against cyber threats, facilitating evidence-based policy formulation and international collaboration.

While several global indices exist, they often lack dynamic, multi-source integration or predictive capability. This study addresses this gap by proposing a data-driven, graph-enhanced NCRI framework that captures both technical and socio-organizational dimensions of resilience.

1.2 Objective and Scope of the National Cyber Resilience Index

This document outlines a data-driven framework for a National Cyber Resilience Index (NCRI). The NCRI intends to provide a quantifiable, dynamic assessment of a nation's capacity to withstand, adapt to, and recover from cyberattacks. It aims to transcend static cybersecurity maturity models by incorporating real-time data analytics and a systems thinking approach. The index will integrate various data sources, including technical infrastructure metrics, policy frameworks, human capital development, and incident response capabilities, to produce a multi-dimensional resilience score. The scope of this index extends to capturing resilience across multiple dimensions, encompassing both preventative measures and adaptive response mechanisms. It considers not only the technical robustness of systems but also the organizational and societal elements that contribute to overall national resilience [5]. Specifically, the NCRI aims to:

- Provide a comprehensive and granular assessment of national cyber resilience.
- Enable benchmarking against international standards and peer nations [3].
- Identify specific areas of strength and weakness within a nation's cyber resilience posture [3].
- Inform strategic resource allocation and policy development for enhancing national cyber preparedness [2].
- Facilitate the integration of diverse, heterogeneous data sources into a cohesive analytical framework [6].

This framework moves beyond traditional, static assessments to incorporate dynamic, data-driven insights for a more adaptive and responsive measure of national cyber resilience.

1.3 Structure of the Paper

This document is organized into five primary sections. Following this introduction, the "Methodology" section details the research approach, covering data sources, framework development, and index construction techniques. The "Literature Review / Thematic Analysis" then surveys existing research and conceptual models pertinent to cyber resilience, its measurement, and the challenges associated with multi-source data

integration. The "Analysis / Discussion" section synthesizes these insights, presenting the proposed NCRI framework, discussing its implications for policy and strategy, and acknowledging its limitations. Finally, the "Conclusion" summarizes key findings, offers recommendations for various stakeholders, and identifies avenues for future research and development in this domain.

The paper is structured as follows: Section 2 explains the methodology; Section 3 reviews key literature; Section 4 presents the proposed framework and analytical approach; Section 5 discusses policy implications and limitations; Section 6 concludes with recommendations and future research directions

2 Methodology

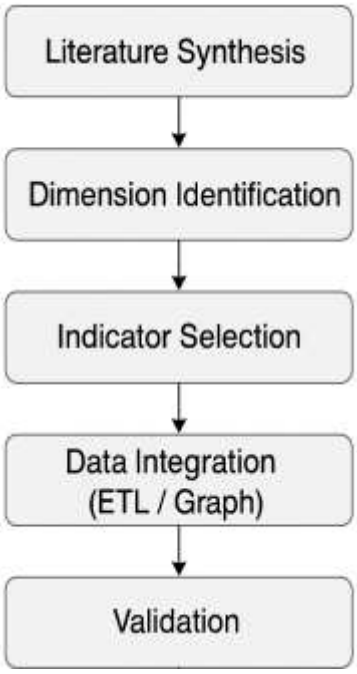
2.1 Research Design and Data Sources

The research design for developing the National Cyber Resilience Index (NCRI) employs a mixed-methods approach, combining systematic literature review with conceptual framework development and data-driven modeling. This hybrid strategy ensures a foundation in established theory and practice while accommodating the dynamic nature of cyber resilience. A systematic literature review process, involving a structured search strategy and explicit inclusion criteria, was initially conducted to identify relevant research on cyber resilience, national security, data integration, and index construction. Data extraction focused on study objectives, methodologies, data sources, analytical techniques, and identified limitations. This systematic appraisal enhances the reliability of the conclusions drawn. Primary data sources for the NCRI will include a variety of publicly available and restricted-access datasets. These encompass:

- **Government Reports:** National cybersecurity strategies, policy documents, and threat assessments.
- **International Indices:** Data from existing global cybersecurity and resilience indices (e.g., Global Cybersecurity Index, National Cyber Security Index) [3].
- **Technical Metrics:** Data on internet penetration, critical infrastructure vulnerabilities, incidence of cyberattacks, and security spending.
- **Legal and Regulatory Frameworks:** Information on cybercrime legislation, data protection laws, and compliance mechanisms.
- **Human Capital Data:** Statistics on cybersecurity workforce, education programs, and public awareness campaigns.
- **Open-Source Intelligence:** Analysis of cyber threat intelligence feeds, dark web activity, and breach disclosures.

The integration of such diverse data is paramount, necessitating robust Extract, Transform, Load (ETL) processes and advanced analytical techniques to handle heterogeneity and ensure data quality [6].

Figure 1: Methodological Overview for NCRI Construction



This figure illustrates the sequential workflow employed in developing the National Cyber Resilience Index (NCRI). The process begins with a systematic literature synthesis, which identifies theoretical foundations and best practices from existing resilience frameworks. These insights guide the dimension identification stage, where core areas of national cyber resilience such as governance, technical capability, and collaboration are defined. Subsequently, the indicator selection phase operationalizes these dimensions into measurable variables supported by accessible datasets. The model then advances to data integration, using ETL (Extract, Transform, Load) and graph-based methods to unify heterogeneous data streams into a cohesive analytical structure. The final validation phase ensures the robustness of the model through expert review, statistical verification, and benchmarking. This workflow underscores the study's rigorous, data-driven approach to measuring national cyber preparedness.

2.2 Framework Development Approach

The framework development for the NCRI adopts a multi-layered, iterative approach, drawing upon principles of systems thinking and organizational resilience [7]. This approach acknowledges the interconnectedness of various components within a national cyber ecosystem. Initial conceptualization involves identifying key dimensions of national cyber resilience based on a synthesis of literature and existing frameworks. These dimensions are then disaggregated into measurable indicators, ensuring their relevance, reliability, and data availability. The framework will incorporate a balanced scorecard methodology, allowing for a comprehensive view across strategic areas [8]. This involves defining specific metrics for each indicator and assigning weights based on expert consensus and sensitivity analysis. The process includes:

1. **Dimension Identification:** Defining broad categories like Governance, Technical Capabilities, Human Capital, and Collaboration.
2. **Indicator Selection:** Specifying quantifiable or qualifiable metrics within each dimension (e.g., number of certified cybersecurity professionals, frequency of cyber drills, legal response times).
3. **Data Mapping:** Linking indicators to available data sources and addressing potential gaps.
4. **Weighting Scheme:** Developing a transparent weighting system for indicators and dimensions, possibly using analytical hierarchy process (AHP) or expert elicitation.
5. **Normalization:** Standardizing disparate data types to enable aggregation and comparison.
6. **Iterative Refinement:** Continuous feedback loops and validation with experts and stakeholders to ensure the framework's practical utility and theoretical soundness.

The aim is to create a framework that is both rigorous and adaptable, capable of evolving with the threat landscape and technological advancements.

2.3 Index Construction and Validation Techniques

The construction of the National Cyber Resilience Index (NCRI) involves several methodical steps to ensure its robustness and interpretive utility. After identifying dimensions and indicators, raw data from various sources undergo preprocessing, including cleansing, transformation, and normalization to a common scale. This step is critical given the heterogeneity of data types, ranging from quantitative statistics to qualitative assessments converted into numerical scores. Aggregation techniques will then combine these normalized indicator scores into sub-dimension scores, and subsequently into overall dimension scores, culminating in a composite NCRI score. The choice of aggregation method (e.g., arithmetic mean, geometric mean, or weighted sum) will be determined during the framework's refinement, considering the interdependencies and relative importance of different components. Validation of the NCRI will employ a multi-pronged approach:

- **Content Validity:** Expert review panels will assess whether the chosen dimensions and indicators comprehensively cover the domain of national cyber resilience. This involves ensuring alignment with established theoretical constructs and best practices in cybersecurity and resilience [9].
- **Construct Validity:** Statistical methods, such as principal component analysis (PCA) or factor analysis, will verify that indicators load onto their intended dimensions, confirming the underlying structure of the index. Correlation with other established national indices (e.g., economic development, innovation indices) will also be examined, where appropriate [3].
- **Predictive Validity:** Where feasible, the NCRI scores will be tested against real-world outcomes, such as reported severity of cyber incidents or recovery times, to

evaluate its ability to predict national performance in cyber resilience [10]. This is challenging due to data secrecy around cyberattacks [10].

- **Sensitivity Analysis:** Varying the weights of indicators and dimensions will determine the stability of the overall index score and identify critical factors that disproportionately influence the outcome.
- **Benchmarking:** Comparison with existing national and international frameworks will provide external validation and context for the NCRI's results.

This rigorous validation process ensures the NCRI is a reliable, meaningful, and actionable tool for assessing national cyber resilience.

2.4 Validation and Benchmarking Workflow

The validation and benchmarking of the NCRI framework employ a hybrid methodology integrating quantitative and qualitative techniques. Following indicator aggregation and normalization, benchmark comparisons will be conducted against existing indices such as the Global Cybersecurity Index (GCI) and the National Cyber Security Index (NCSI).

Correlation Analysis: Pearson or Spearman correlation coefficients will assess how closely NCRI scores align with established benchmarks across participating countries.

Principal Component Analysis (PCA): PCA will test the dimensional integrity of indicators, confirming whether grouped metrics coherently represent the intended resilience constructs.

Cross-Validation: Historical cyber incident data will be used to assess predictive validity whether higher NCRI scores correlate with lower incident severity or faster recovery rates.

Sensitivity Testing: Monte Carlo simulations will evaluate how changes in indicator weights affect the stability of overall scores, ensuring robustness.

Together, these steps ensure the NCRI remains both empirically sound and policy-relevant, offering reliable insights into national cyber posture.

3 Literature Review / Thematic Analysis

3.1 The Evolution of Cyber Resilience Concepts

3.1.1 From Cybersecurity to Cyber Resilience

The conceptual landscape surrounding digital protection has undergone a significant transformation, moving from a primary focus on cybersecurity to a broader embrace of cyber resilience. Initially, cybersecurity efforts concentrated on preventative measures, aiming to erect impenetrable defenses against external threats. This approach, while foundational, proved increasingly inadequate as the threat landscape evolved, characterized by sophisticated and persistent adversaries [1]. The inevitability of breaches necessitated a shift towards a more adaptive strategy. Cyber resilience acknowledges that perfect prevention is unattainable and that cyber incidents will occur [1]. Consequently,

the emphasis expands to include an organization's or nation's ability to prepare for, absorb, recover from, and adapt to disruptive cyber events while maintaining essential functions [1] . This paradigm shift is rooted in the broader concept of resilience, which involves adapting to disruptions that threaten existence [11]. For individuals, cyber resilience involves the ability to resist or rapidly recover from attacks [9]. For organizations, it means mobilizing expertise and resources to combat the effects of cyberattacks on business operations [7]. The integration of cyber resilience into national strategies reflects a recognition that robust digital infrastructure must be capable of enduring and adapting to continuous cyber challenges.

3.1.2 International Standards and Assessment Frameworks

Several international standards and assessment frameworks have emerged to guide and measure cyber resilience, reflecting a collective effort to standardize practices and facilitate comparison across entities. These frameworks often define the typical characteristics of cyber resilience, detailing its concept and outlining the link between cybersecurity and resilience. Prominent examples include the Cyber Resilience Review (CRR), the Cyber Perception Index (CRF), and the Cyber Risk Index (CRI), which represent global methods for assessing cyber resilience. Beyond these, various maturity models contribute to assessing the security level of a system or organization [12][4]. These models typically provide a structured approach for evaluating an entity's capabilities across different domains, such as governance, risk management, and incident response. For critical infrastructure, a systems thinking approach has been proposed to explore cyber resilience as a system property, with expressions relating to operational dimensions and domains of practice. This approach considers infrastructure and services within their sectoral system context, viewing them as a system of systems. Such frameworks provide a basis for identifying strengths and weaknesses, offering strategic guidance for organizations to embed cyber resilience within digital transformation initiatives. The development of national cybersecurity strategies and action plans often incorporates these methodologies, with a growing intention to include effectiveness indicators that measure net benefits against implementation costs. Despite these advancements, a universal understanding of resilience remains elusive across disciplines due to varied definitions and measurement approaches [11].

3.2 Quantitative and Data-Driven Approaches

3.2.1 Quantitative Measurement Methodologies

Quantitative measurement methodologies for cyber resilience frequently leverage metrics and statistical analysis to provide empirical assessments. These approaches move beyond qualitative descriptions to offer measurable insights into an entity's ability to resist, detect, and recover from cyber threats. For instance, enterprise resilience can be enhanced through data analytics, employing system monitoring data combined with data mining and machine learning techniques to proactively detect potential disruptions [13]. This enables intelligent business analytics systems to assist operational teams in improving resilience [13]. In a broader context, disaster resilience indices often incorporate a multitude of quantitative factors. One such example includes analyzing over 20,000 historical disaster data points from 207 countries, considering 6 primary indices and 38

secondary influencing factors (e.g., disaster frequency, population density, GDP) to calculate a country's resilience score [14]. These analyses reveal critical factors affecting resilience and allow for comprehensive comparisons [14]. Similarly, public transit networks' resilience and vulnerability during natural disasters have been quantified using diverse traffic, infrastructure, events, and web-based big data sources [15]. Performance measures such as critical link identification, change in travel time, and "resilience triangles" are estimated to assess recovery and plan for future disasters [15]. These methodologies underscore the utility of data-driven approaches in revealing patterns and correlations that traditional methods might overlook. The application of machine learning, for example, permits dynamic adjustments to models based on evolving data patterns, moving beyond static, rule-based systems to more adaptive services. Metrics for evaluating model performance, such as precision, recall, F1-score, AUROC, and AUPRC, are routinely employed in fraud detection and other security contexts, providing a robust framework for assessing the effectiveness of data-driven solutions.

3.2.2 Maturity Models and Sectoral Indices

Maturity models and indices serve as structured assessment tools for evaluating cyber resilience at various scales, from individual organizations to entire nations and specific sectors. These models typically provide a phased approach, detailing different levels of capability or preparedness. For instance, the Cyber Resilience Review (CRR) and the Cyber Perception Index (CRF) are prominent global methods for assessing cyber resilience, offering insights into a nation's ability to manage cyber risks. Such indices often position countries by their level of development in the global space, identifying strengths and weaknesses in cybersecurity management [3]. At the national level, the evaluation of cybersecurity maturity often involves developing bespoke models. An example includes a national cyber security maturity measurement model created using a mixed-methods approach and content analysis, selecting key components and criteria based on expert opinions [4]. The results of such models are then compared with other research models to highlight advantages [4]. Furthermore, the Global Cybersecurity Index (GCI) and National Cyber Security Index (NCSI) are utilized as component indices to characterize the potential of the digital economy and a country's participation in cybersecurity [3]. A correlation between GCI, information society development indices, and GDP per capita confirms that digital transformation, when coupled with assured information and cybersecurity, drives economic development [3]. For sectoral applications, cyber resilience maturity models are being developed for critical infrastructure, employing a systems thinking perspective to assess resilience across operational dimensions and practice domains. This approach frames a set of expressions designed to probe the sectoral design space and serve as design considerations for improving cyber resilience. These efforts collectively demonstrate a movement towards more sophisticated and context-specific evaluations of cyber resilience, recognizing that generic application of frameworks is often inappropriate [11].

3.3 Challenges in Data Integration

3.3.1 Multi-Source Data Collection and ETL Processes

Constructing a National Cyber Resilience Index necessitates integrating data from numerous, heterogeneous sources, which introduces significant challenges for data collection and Extract, Transform, Load (ETL) processes. The diverse nature of national cyber resilience data includes technical logs, policy documents, survey results, and geopolitical intelligence, each with distinct formats, structures, and update frequencies. This heterogeneity frequently creates structural and semantic integration problems that require specific solutions [6]. Effective ETL processes are crucial for converting raw data into a usable format for analysis. However, the complexity of multi-source data integration directly influences the performance and reliability of these pipelines. Highly complex transformations, particularly those involving extensive data cleansing, entity resolution, and semantic mapping across large datasets, can become computationally intensive, leading to increased processing time and resource consumption. Moreover, dependencies on multiple source systems introduce numerous points of failure; an outage or data anomaly in one source can disrupt the entire ingestion pipeline, compromising data freshness and integrity. The emergence of graph-centric ETL approaches addresses some of these limitations, especially when dealing with interconnected data. These methodologies recognize the inherent graph structure from the outset, designing transformations that directly map source data into nodes, edges, and properties. This shifts the focus from tabular joins to identifying entities and their relationships, often requiring a semantic understanding of the data. Tools and frameworks supporting graph-specific data models during transformation allow for more intuitive and efficient representation of interconnected information.

3.3.2 Scalability, Interoperability, and Data Quality Issues

Scalability, interoperability, and data quality represent critical hurdles in constructing national cyber resilience indices. The sheer volume and velocity of data generated across a nation's cyber ecosystem necessitate scalable ETL solutions that can handle increasing data volumes and incorporate new sources without becoming bottlenecks. Without proper scalability, data ingestion can impede the ability to continuously update and refine the index. Interoperability issues arise from the disparate systems and formats used by various government agencies, private sectors, and international partners. Achieving semantic interoperability where data from different sources can be meaningfully combined and interpreted often demands sophisticated mapping and harmonization efforts. The MIDAS platform, for example, connects many isolated heterogeneous data sources, combining rich datasets for application of analytics, monitoring, and research tools, demonstrating a pathway for overcoming such challenges [16]. Data quality concerns are pervasive. Inconsistencies, missing values, inaccuracies, and timeliness issues can severely compromise the reliability and validity of an index. Data cleansing and validation routines are essential to mitigate these risks. Furthermore, the sensitivity of cybersecurity data often introduces access and sharing restrictions, complicating comprehensive data collection. Robust ETL processes support data governance and compliance requirements by ensuring data lineage, auditability, and adherence to quality standards. These challenges collectively underscore the necessity for advanced data

engineering and governance strategies to build a credible and effective National Cyber Resilience Index.

The reviewed literature underscores both conceptual maturity and operational fragmentation in resilience measurement, establishing the rationale for a unified NCRI framework integrating multi-source analytics.

Table 1: Comparison of Existing Cyber Resilience Frameworks

Framework / Index	Scope	Methodology	Data Type	Strengths	Limitations
Cyber Resilience Review (CRR)	Organizational	Qualitative maturity model	Survey data	Widely adopted for capability assessment	Lacks real-time adaptability
Global Cybersecurity Index (GCI)	National	Weighted composite scoring	Governmental reports	Enables international comparison	Focuses more on policy than adaptability
National Cyber Security Index (NCSI)	National	Indicator-based scoring	Public policy datasets	Broad country coverage	Limited dynamic updating
Cyber Risk Index (CRI)	Corporate	Quantitative risk rating	Statistical / event data	Integrates economic and risk factors	Not designed for national benchmarking
Cyber Perception Framework (CRF)	Global	Mixed-methods	Survey + quantitative	Captures perception of readiness	Subjective weighting of indicators
Proposed NCRI (This Study)	National / Systemic	Data-driven, graph-enhanced	Heterogeneous datasets	Real-time analytics, predictive capability	Data collection and harmonization challenges

Table 1 demonstrates how the proposed NCRI builds upon prior models by integrating heterogeneous data analytics and predictive modeling for cross-sector resilience measurement.

4 Analysis / Discussion

4.1 Designing a Robust National Cyber Resilience Index Framework

4.1.1 Key Dimensions and Indicators of Cyber Resilience

Designing a robust National Cyber Resilience Index (NCRI) framework necessitates careful consideration of its constituent dimensions and measurable indicators. Drawing upon existing literature and established frameworks, a multi-dimensional approach is essential to capture the multifaceted nature of cyber resilience. Broadly, these dimensions can be categorized into governance, technical capabilities, human capital, and collaboration. Within the governance dimension, indicators could include the existence and maturity of national cybersecurity strategies, clear regulatory frameworks for data protection and incident reporting, and the effectiveness of cybercrime legislation. This encompasses the institutional capacity to develop and enforce policies that foster a secure cyber environment. Technical capabilities involve metrics such as the prevalence of secure network configurations, adoption rates of advanced security technologies, infrastructure redundancy, and the capacity for rapid threat detection and response. This dimension assesses the physical and logical defenses of a nation's digital infrastructure. Human capital evaluates the availability of skilled cybersecurity professionals, the scope and quality of cybersecurity education programs, and public awareness regarding cyber threats and safe online practices [9]. This recognizes that technology alone cannot confer resilience without competent human operation and vigilance. The collaboration dimension measures the extent of information sharing between government agencies, private sector entities, and international partners. This includes participation in joint cyber exercises, intelligence sharing agreements, and public-private partnerships for incident response. Each indicator within these dimensions requires specific, quantifiable metrics. For example, rather than a general "good policy," the framework would assess the number of certified cybersecurity professionals per capita, the average time to detect a breach, or the percentage of critical infrastructure adhering to specific security standards. This granular approach moves beyond subjective assessments to provide an empirically grounded view of national cyber resilience.

Figure 2: Conceptual Architecture of the NCRI Framework

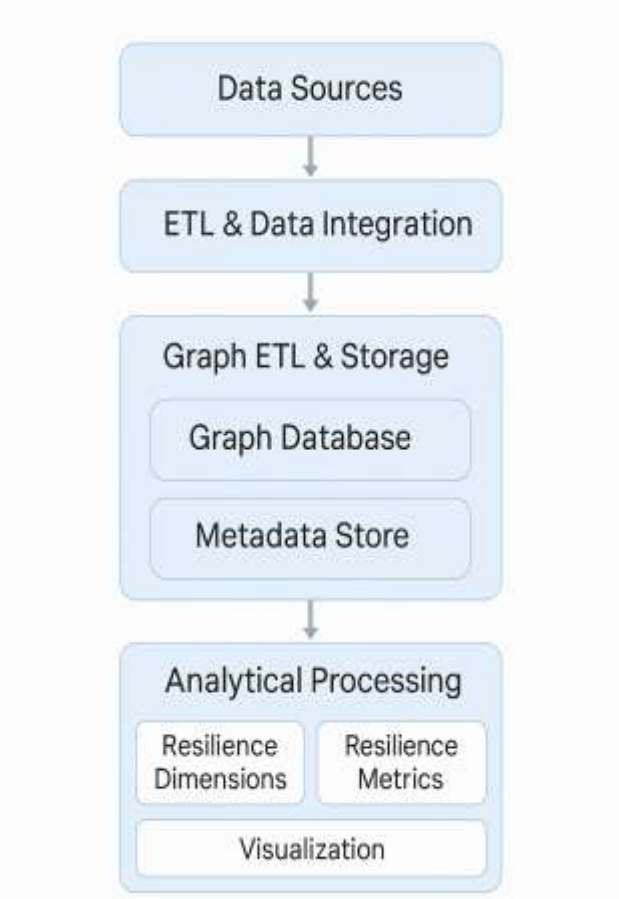


Figure 2 presents the conceptual architecture of the National Cyber Resilience Index (NCRI), structured as a layered system that translates raw data into actionable insights. The base layer Data Sources aggregates information from government reports, technical metrics, legal frameworks, human capital indicators, and open-source intelligence. These inputs flow upward to the ETL and Data Integration layer, where data cleansing, transformation, and normalization ensure consistency and quality. The Graph ETL & Storage layer builds a graph-based data repository linking entities, relationships, and dependencies, enabling relational insights often missed by traditional tabular methods. The Analytical Processing layer leverages these graph structures to calculate resilience metrics across dimensions such as governance, technical strength, and collaboration, producing composite scores and dashboards. Finally, visualization modules present dynamic results for policymakers, allowing for real-time monitoring and continuous improvement. The layered architecture reflects a scalable, adaptive framework capable of evolving with emerging cyber threats and technologies.

4.1.2 Integrating Multi-Source and Graph-Based Data Analytics

Effective implementation of a National Cyber Resilience Index (NCRI) requires advanced data integration and analytical techniques, particularly those capable of handling multi-source, heterogeneous data. Multi-source data collection presents challenges due to variations in format, semantics, and timeliness [6]. The NCRI benefits

significantly from the integration of diverse datasets, including technical logs, incident reports, policy documents, economic indicators, and social media data. Robust Extract, Transform, Load (ETL) pipelines are essential for cleansing, standardizing, and consolidating this information. The performance and reliability of these pipelines are critical, as complex transformations can be computationally intensive and introduce points of failure. Graph-based data analytics offers a powerful paradigm for making sense of the interconnectedness inherent in cyber resilience data. Cyber ecosystems are intrinsically graph-like, with entities (e.g., organizations, individuals, IP addresses, vulnerabilities) connected by relationships (e.g., communication, attack vectors, supply chains). Traditional tabular databases struggle to capture these complex relationships efficiently. Graph databases and Graph Neural Networks (GNNs) provide an architecture where entities (nodes) and their relationships (edges) are primary components, enabling sophisticated analysis of dependencies, influence, and propagation pathways in cyber incidents. Specific benefits of graph-based analytics for the NCRI include:

- **Relationship Mapping:** Identifying critical interdependencies between infrastructure components, organizations, and national assets.
- **Threat Propagation Modeling:** Simulating how cyberattacks might spread across a national network, revealing critical nodes and potential systemic vulnerabilities.
- **Anomaly Detection:** GNNs can identify unusual patterns in network traffic or system behavior that traditional methods might miss.
- **Supply Chain Risk Assessment:** Visualizing and analyzing complex supply chain relationships to identify single points of failure or compromised vendors.
- **Policy Impact Analysis:** Modeling the downstream effects of policy changes on various elements of the cyber ecosystem.

The adoption of graph-centric ETL approaches, which directly map source data into graph structures, facilitates this integration, offering more intuitive and efficient representation of interconnected information. This analytical capability elevates the NCRI from a static scorecard to a dynamic, predictive instrument, offering deeper insights into national cyber resilience.

Figure 3: Graph-Based Analytical Model for National Cyber Resilience

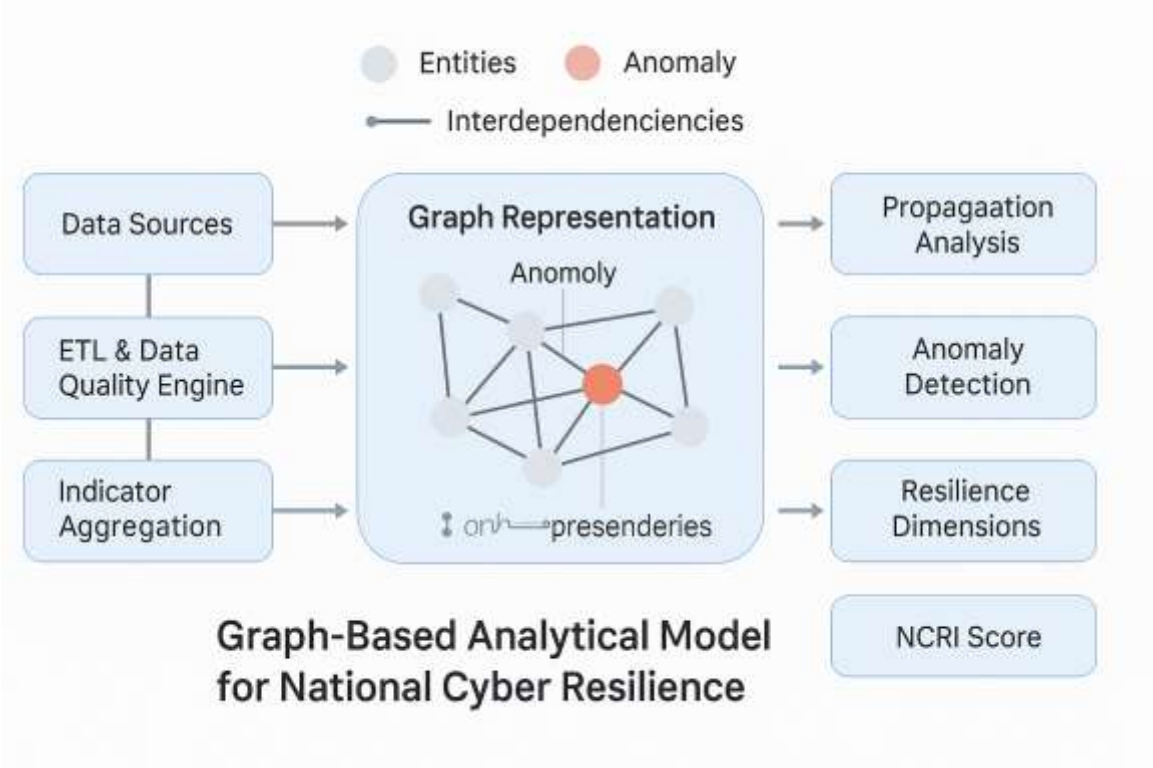


Figure 3 depicts the graph-based analytical model at the core of the NCRI's analytical engine. It visualizes how diverse entities government agencies, infrastructure operators, cybersecurity firms, and citizens are interconnected through data flows and interdependencies. Within the graph representation, each node signifies an entity, while edges capture relationships such as data sharing, dependency, or vulnerability propagation. Anomalies detected in this network (highlighted nodes) indicate potential weaknesses or irregularities that could compromise national cyber resilience. Through integrated analytics modules, the model supports propagation analysis, which simulates how cyberattacks might spread through interlinked systems; anomaly detection, identifying deviations from expected patterns; and policy impact analysis, which predicts how regulatory interventions alter the resilience landscape. Outputs from these analytics feed into the NCRI scoring engine, translating complex network behaviors into interpretable, data-driven resilience indicators. This figure exemplifies how graph-based intelligence transforms static data into dynamic insights for real-time policy action.

4.2 Implications for Policy, Strategy, and Implementation

4.2.1 Operationalization of Cyber Resilience in National Strategies

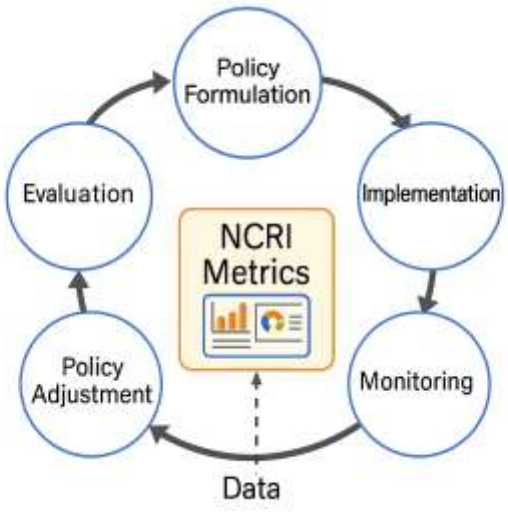
The National Cyber Resilience Index (NCRI) offers substantial implications for the operationalization of cyber resilience within national strategies. By providing a data-driven, quantifiable assessment, the NCRI moves strategic planning beyond reactive measures to a proactive, evidence-based approach. Policymakers can leverage the index to identify specific areas of weakness and strength, allowing for targeted resource

allocation and policy interventions [2]. For instance, a low score in the "human capital" dimension might prompt increased investment in cybersecurity education and training programs, whereas a deficiency in "technical capabilities" could spur initiatives for critical infrastructure modernization. The NCRI facilitates the establishment of measurable goals and key performance indicators (KPIs) for national cybersecurity programs. Instead of generic objectives, strategies can specify quantifiable improvements in resilience scores over time, enabling accountability and progress tracking. This aligns with the intention of including effectiveness indicators as a ratio of net benefits and implementation costs, as observed in some national strategy development processes. Furthermore, the framework supports a continuous improvement cycle. Regular assessment via the NCRI permits nations to adapt their strategies in response to evolving threats and technological advancements. This adaptive approach is crucial given the dynamic nature of the cyber threat landscape. The index's capacity to integrate multi-source and graph-based data analytics offers real-time insights, enabling quicker adjustments to operational strategies and incident response protocols. This operationalization fosters a more agile and responsive national cyber defense posture, aligning with the principles of organizational ambidexterity in cybersecurity [8].

Regular assessment via the NCRI permits nations to adapt their strategies in response to evolving threats and technological advancements. This adaptive approach is crucial given the dynamic nature of the cyber threat landscape. The index’s ability to provide real-time insights supports evidence-based decision-making and continuous policy refinement.

Figure 4 depicts the NCRI’s policy feedback mechanism, where index outcomes directly inform the iterative process of national cybersecurity planning and evaluation

Figure 4. Policy and Impact Feedback Loop for the National Cyber Resilience Index



This figure illustrates the cyclical relationship between policy formulation, implementation, monitoring through NCRI metrics, evaluation, and subsequent policy adjustment. The feedback loop emphasizes continuous improvement, where NCRI data

provides evidence to guide decision-making, optimize investments, and align national resilience strategies with evolving threat landscapes.

4.2.2 Societal, Economic, and Organizational Impacts

The implementation and continuous monitoring of a National Cyber Resilience Index (NCRI) extend far beyond technical metrics, yielding significant societal, economic, and organizational impacts. Societally, an enhanced national cyber resilience translates directly into increased public trust in digital services, from e-governance to online banking. This fosters a more secure digital environment for citizens, reducing their vulnerability to cybercrime and data breaches [9]. Furthermore, an NCRI can inform public awareness campaigns and national education initiatives, thereby improving overall cyber hygiene among the populace. Economically, a high NCRI score signals a secure digital economy, attracting foreign investment and stimulating innovation. It minimizes the economic disruption caused by cyberattacks, which can result in substantial financial losses, reputational damage, and operational downtime. For example, by effectively disrupting illicit financial networks, Graph Neural Networks (GNNs) contribute directly to undermining the economic foundations of criminal enterprises, leading to a safer global environment. Moreover, the NCRI's ability to benchmark a nation's cyber posture can influence its standing in the global digital economy, potentially affecting trade relations and international partnerships. Organizationally, the NCRI can serve as a catalyst for internal improvements across various sectors. Organizations within a nation will likely align their own cyber resilience efforts with national priorities, seeking to improve their individual contributions to the overall index score. This fosters a harmonized approach to cybersecurity, encouraging best practices and the adoption of robust frameworks. The emphasis on data-driven decision-making can also lead to more efficient resource allocation within organizations, promoting a culture of continuous security improvement. Managers' perceptions of cyber risks, when informed by comprehensive national assessments, can drive the adoption of effective cyber resilience strategies within supply chains. The NCRI, therefore, acts as a feedback mechanism, driving positive change across all levels of a nation's digital ecosystem.

Table 2: Key Dimensions, Indicators, and Example Metrics

Dimension	**Indicators**	**Example Metrics / Data Sources**
Governance	National cybersecurity strategy, legislative framework, institutional coordination	Number of enacted cyber laws, response time of national CERT, budget share for cybersecurity
Technical Capabilities	Threat detection, incident response, network redundancy	Mean time to detect/respond (MTTD/MTTR), % critical infrastructure with ISO 27001 certification

Human Capital	Workforce development, awareness programs, academic capacity	Number of certified professionals per capita, cybersecurity degrees offered, public awareness scores
Collaboration	Public–private partnerships, international cooperation	Number of joint cyber drills, bilateral threat-sharing agreements, participation in international forums

Table 2 illustrates the NCRI's balanced structure, combining governance, technical, human, and collaborative elements to form a holistic measure of national cyber resilience

4.3 Limitations and Future Directions in Cyber Resilience Measurement

Despite its potential, the National Cyber Resilience Index (NCRI) framework faces inherent limitations. Data availability and reliability pose a significant challenge; collecting comprehensive, accurate, and timely data across diverse national sectors can be difficult due to proprietary concerns, classification, and varying reporting standards. The secrecy surrounding cyberattacks and how organizations manage their cyber resilience often hinders a complete understanding of actual resilience levels [10]. Furthermore, the dynamic nature of cyber threats means that any index, no matter how sophisticated, risks becoming outdated if not continuously updated and refined. The weighting of indicators and dimensions, while informed by expert opinion, can introduce subjectivity, potentially affecting the index's perceived objectivity. Finally, while technical efficacy of models is often showcased, rigorous evaluation of their long-term behavioral impact on actual habits is less common. The interaction between personality traits, financial literacy, and data-driven interventions could benefit from more nuanced exploration. Future research and development efforts for cyber resilience measurement should concentrate on several key areas:

1. **Real-time Data Integration and Predictive Analytics:** Developing more sophisticated mechanisms for real-time data ingestion and predictive modeling, potentially leveraging advanced machine learning to anticipate emerging threats and vulnerabilities.
2. **Granular Impact Assessment:** Moving beyond general resilience scores to provide more granular insights into the impact of cyber incidents on specific sectors or critical functions. This includes exploring methods for assessing the long-term behavioral impacts of systems beyond mere financial efficiency.
3. **Standardization of Reporting:** Advocating for international standards in cyber incident reporting and data sharing to enhance cross-national comparability and data quality.
4. **Ethical and Privacy Considerations:** Deep empirical investigation into the ethical dimensions of alternative data use, particularly concerning privacy,

algorithmic transparency, and bias mitigation. Comprehensive frameworks for auditing and ensuring fairness in data-driven systems remain underdeveloped.

5. **Longitudinal Studies:** Conducting longitudinal studies that track changes in behavior beyond immediate responses to assess the sustained effect of data-driven interventions.
6. **Adaptive Interventions:** Prioritizing the development and rigorous evaluation of adaptive, personalized interventions that leverage real-time data to foster resilient habits.
7. **Scalability of Graph Analytics:** Enhancing the scalability of Graph Neural Networks (GNNs) for ultra-large graphs, possibly through novel sampling techniques or distributed computing paradigms, and developing GNN architectures for dynamic graphs capable of real-time adaptation.
8. **Explainable AI for Transparency:** Investing in transparent AI systems that explain decisions to consumers, addressing concerns about algorithmic black boxes.

Addressing these limitations and pursuing these research avenues will refine the accuracy and utility of national cyber resilience measurement tools.

4.3.1 Emerging Research Directions - Quantum-Safe Encryption and Standardized Resilience Metrics

Future iterations of the NCRI can integrate quantum-resistant cryptography to strengthen national preparedness against post-quantum threats. As quantum computing advances, existing cryptographic systems RSA and ECC become vulnerable. Developing quantum-safe encryption protocols, such as lattice-based or hash-based cryptography, will be essential for sustaining trust in digital infrastructures.

Additionally, there is a growing call for standardized resilience metrics that quantify performance and recovery within graph ETL pipelines. These metrics could measure latency, data loss, and node connectivity stability during simulated attacks or node failures. Establishing such standards will allow nations to evaluate cyber resilience consistently and facilitate interoperability between analytical systems.

4.4 Ethical, Privacy, and Explainability Considerations

The adoption of a data-driven NCRI necessitates a strong ethical and governance framework to protect individual rights and ensure accountability. Three principles guide ethical implementation:

1. Privacy Preservation: Sensitive datasets must undergo anonymization and adhere to data minimization practices consistent with international privacy standards such as GDPR and NIST Privacy Framework.
2. Algorithmic Transparency: Machine-learning and graph-based analytics used within the NCRI should provide interpretable outputs. Explainable AI (XAI) mechanisms such as SHAP or attention visualization must clarify how particular indicators contribute to the final score.

3. Bias Mitigation: Training data must be audited for systemic bias to prevent skewed national comparisons, particularly where low-income nations face limited data availability.

A public-facing dashboard should disclose data provenance, model parameters, and performance metrics to build public trust.

5 Conclusion

5.1 Summary of Findings and Contributions

This study contributes a structured, data-driven NCRI framework that can serve as a benchmark tool for policymakers, researchers, and industry leaders seeking to evaluate and strengthen national preparedness.

This document has presented a comprehensive, data-driven framework for a National Cyber Resilience Index (NCRI), building upon the evolving understanding of cyber resilience as a multi-faceted concept extending beyond traditional cybersecurity. A systematic review of literature highlighted the shift from purely preventative measures to an adaptive approach that encompasses preparing for, absorbing, recovering from, and adapting to cyber incidents [1]. Existing international standards and national maturity models provide a foundation, yet a need persists for a more integrated, dynamic, and data-intensive assessment tool [4]. The proposed NCRI framework integrates key dimensions such as governance, technical capabilities, human capital, and collaboration, each supported by specific, measurable indicators. A significant contribution lies in advocating for the integration of multi-source and graph-based data analytics. This methodology addresses the inherent complexity and interconnectedness of cyber ecosystems, enabling a more dynamic and predictive assessment of national resilience by mapping relationships, modeling threat propagation, and detecting anomalies. The approach acknowledges and seeks to mitigate challenges associated with multi-source data collection, ETL processes, scalability, interoperability, and data quality. The NCRI, therefore, offers a novel synthesis of theoretical understanding and practical data science application, providing a robust instrument for national cyber preparedness.

5.2 Recommendations for Stakeholders and Policymakers

The development and implementation of a National Cyber Resilience Index (NCRI) carry significant implications for various stakeholders and policymakers, necessitating targeted recommendations: For **Policymakers and National Security Agencies**:

1. **Legislate Data Sharing Standards:** Establish clear legal and regulatory frameworks for secure, standardized data sharing across government entities and critical private sectors to improve data availability and quality for the NCRI.
2. **Integrate NCRI into National Strategy:** Embed the NCRI as a core metric within national cybersecurity strategies, using its findings to prioritize investments, allocate resources, and measure progress against defined resilience goals.

3. **Promote Public-Private Partnerships:** Foster collaborative initiatives that enable data exchange and joint exercises, enhancing collective resilience and providing richer data inputs for the index.
4. **Develop Human Capital:** Invest in national cybersecurity education, training, and awareness programs to cultivate a skilled workforce and a cyber-aware citizenry, directly impacting the "human capital" dimension of the NCRI.

For **Industry and Critical Infrastructure Operators**:

1. **Align with National Frameworks:** Harmonize internal cybersecurity and resilience practices with national NCRI dimensions and indicators, contributing to a cohesive national posture.
2. **Invest in Data Infrastructure:** Prioritize investments in robust data collection, ETL processes, and analytics capabilities to support comprehensive and timely reporting, recognizing the intricate nature of multi-source data integration.
3. **Participate in Information Sharing:** Actively engage in cyber threat intelligence sharing platforms and collaborative forums to enhance collective situational awareness and improve NCRI data inputs.

For **Researchers and Academia**:

1. **Advance Data Analytics:** Continue developing cutting-edge graph-based analytics, machine learning, and AI techniques for real-time threat intelligence and predictive resilience modeling.
2. **Address Ethical Considerations:** Conduct further research into the ethical implications of data collection, algorithmic bias, and privacy issues within data-driven resilience frameworks, ensuring robust regulatory and transparent practices.

These recommendations aim to facilitate the effective operationalization of the NCRI, enhancing national cyber resilience across all sectors.

This study contributes a structured, data-driven NCRI framework that can serve as a benchmark tool for policymakers, researchers, and industry leaders seeking to evaluate and strengthen national preparedness.

5.3 Pathways for Future Research and Development

Future research and development efforts stemming from the National Cyber Resilience Index (NCRI) framework can significantly advance the field of national cyber preparedness. A primary pathway involves enhancing the index's predictive capabilities. This includes exploring novel machine learning models, particularly Graph Neural Networks (GNNs), that can process vast, interconnected datasets to forecast emerging threats and identify potential cascading failures within national critical infrastructure. Research into robust adversarial training techniques for GNNs can also enhance their resilience against sophisticated evasion strategies. Another important area concerns the refinement of data integration methodologies. Further work on semantic interoperability and automated data harmonization across disparate national and international sources can reduce manual effort and improve data quality. This involves developing more advanced

ETL tools capable of handling the volume and complexity of cyber resilience data. Investigating the integration of GNNs with other AI modalities, such as natural language processing for analyzing unstructured transaction descriptions, could offer a more holistic approach to threat detection. The socio-technical aspects of cyber resilience also warrant deeper exploration. This includes longitudinal studies to assess the sustained behavioral impact of data-driven interventions on national cyber hygiene and individual resilience. Research could also focus on the effectiveness of dynamic feedback loops that adjust based on individual progress and learning styles, optimizing the frequency, channel, and content of data-driven advice. Furthermore, the development of explainable AI (XAI) for the NCRI is crucial to ensure transparency and trust in the index's outcomes, particularly concerning algorithmic bias and the ethical implications of data usage. Finally, comparative analyses of different intervention types, particularly those combining financial incentives with behavioral nudges, can identify optimal strategies for promoting lasting financial wellbeing and broader cyber resilience. These avenues collectively strive to make the NCRI a more accurate, adaptive, and impactful tool for safeguarding national digital assets.

References

[1] S. M. Alhidaifi, M. R. Asghar, and I. S. Ansari, "A Survey on Cyber Resilience: Key Strategies, Research Challenges, and Future Directions," *ACM Computing Surveys*, vol. 56, no. 8. Association for Computing Machinery (ACM), pp. 1–48, Apr. 26, 2024. doi: 10.1145/3649218.

[2] A. Kott and I. Linkov, "To Improve Cyber Resilience, Measure It," *Computer*, vol. 54, no. 2. Institute of Electrical and Electronics Engineers (IEEE), pp. 80–85, Feb. 2021. doi: 10.1109/mc.2020.3038411.

[3] A. Yerina, I. Honchar, and S. Zaiets, "Statistical Indicators of Cybersecurity Development in the Context of Digital Transformation of Economy and Society," *Science and Innovation*, vol. 17, no. 3. National Academy of Sciences of Ukraine (Co. LTD Ukrinformnauka) (Publications), pp. 3–13, Jun. 17, 2021. doi: 10.15407/scine17.03.003.

[4] M. Omrani, M. Shafiee, and S. Khorsandi, "A Model to Measure Cyber Security Maturity at the National Level," *2023 31st International Conference on Electrical Engineering (ICEE)*. IEEE, pp. 110–116, May 09, 2023. doi: 10.1109/icee59167.2023.10334826.

[5] M. F. Safitra, M. Lubis, and M. T. Kurniawan, "Cyber Resilience: Research Opportunities," *Proceedings of the 2023 6th International Conference on Electronics, Communications and Control Engineering*. ACM, pp. 99–104, Mar. 24, 2023. doi: 10.1145/3592307.3592323.

[6] E. A. Merieme, A. Mohamed, C. Ali, Y. Fakhri, and G. Noreddine, "A survey on the challenges of data integration," *2022 9th International Conference on Wireless Networks and Mobile Communications (WINCOM)*. IEEE, pp. 1–6, Oct. 26, 2022. doi: 10.1109/wincom55661.2022.9966419.

[7] G. Appiah, J. Amankwah-Amoah, and Y.-L. Liu, "Organizational Architecture, Resilience, and Cyberattacks," *IEEE Transactions on Engineering Management*, vol. 69,

no. 5. Institute of Electrical and Electronics Engineers (IEEE), pp. 2218–2233, Oct. 2022. doi: 10.1109/tem.2020.3004610.

[8] E. G. Carayannis, E. Grigoroudis, S. S. Rehman, and N. Samarakoon, "Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience," *IEEE Transactions on Engineering Management*, vol. 68, no. 1. Institute of Electrical and Electronics Engineers (IEEE), pp. 223–234, Feb. 2021. doi: 10.1109/tem.2019.2909909.

[9] A. N. Joinson, M. Dixon, L. Coventry, and P. Briggs, "Development of a new 'human cyber-resilience scale,'" *Journal of Cybersecurity*, vol. 9, no. 1. Oxford University Press (OUP), Jan. 01, 2023. doi: 10.1093/cybsec/tyad007.

[10] E. Tsen, R. K. L. Ko, and S. Slapnicar, "An exploratory study of organizational cyber resilience, its precursors and outcomes," *Journal of Organizational Computing and Electronic Commerce*, vol. 32, no. 2. Informa UK Limited, pp. 153–174, Apr. 03, 2022. doi: 10.1080/10919392.2022.2068906.

[11] S. Kativhu, M. Mwale, and J. Francis, "Approaches to measuring resilience and their applicability to small retail business resilience," *Problems and Perspectives in Management*, vol. 16, no. 4. LLC CPC Business Perspectives, pp. 275–284, Nov. 28, 2018. doi: 10.21511/ppm.16(4).2018.23.

[12] N. T. Le and D. B. Hoang, "Can maturity models support cyber security?," *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*. IEEE, pp. 1–7, Dec. 2016. doi: 10.1109/pccc.2016.7820663.

[13] D. Xu, I. W. Tsang, E. K. Chew, C. Siclari, and V. Kaul, "A Data-Analytics Approach for Enterprise Resilience," *IEEE Intelligent Systems*, vol. 34, no. 3. Institute of Electrical and Electronics Engineers (IEEE), pp. 6–18, May 01, 2019. doi: 10.1109/mis.2019.2918092.

[14] N. Zhang and H. Huang, "Resilience Analysis of Countries under Disasters Based on Multisource Data," *Risk Analysis*, vol. 38, no. 1. Wiley, pp. 31–42, Apr. 06, 2017. doi: 10.1111/risa.12807.

[15] S. Mudigonda, K. Ozbay, and B. Bartin, "Evaluating the resilience and recovery of public transit system using big data: Case study from New Jersey," *Journal of Transportation Safety & Security*, vol. 11, no. 5. Informa UK Limited, pp. 491–519, Mar. 26, 2018. doi: 10.1080/19439962.2018.1436105.

[16] J. Pita Costa *et al.*, "Meaningful Big Data Integration for a Global COVID-19 Strategy," *IEEE Computational Intelligence Magazine*, vol. 15, no. 4. Institute of Electrical and Electronics Engineers (IEEE), pp. 51–61, Nov. 2020. doi: 10.1109/mci.2020.3019898.