ISA Journal of Engineering and Technology (ISAJET)

Homepage: https://isapublisher.com/isajet/
Email: office.isapublisher@gmail.com

Volume 2, Issue 6, Nov-Dec, 2025 ISSN: 3049-1843

The Adaptive Organizational Cybersecurity Maturity Model (AOCMM): A Design Science Approach for Critical National Infrastructure

Abdul-Malik Suleiman, Mbanaso Uche M., Steven I. Bassey, Gilbert I.O. Aimufua

Center for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria

Received: *30.10.2025* **|** ***Accepted:*** *28.11.2025* **|** ***Published:*** *30.11.2025*

***Corresponding Author:** Abdul-Malik Suleiman

DOI: *10.5281/zenodo.17769400*

Abstract **Original Research Article**

Cybersecurity threats represent a persistent and escalating operational risk, particularly for Critical National Infrastructure (CNI) [1]. Existing cybersecurity maturity models often lack the necessary adaptability and intelligence to keep pace with the perpetually evolving threat landscape [2] [3]. This paper introduces the Adaptive Organizational Cybersecurity Maturity Model (AOCMM), an innovative framework developed using the Design Science Research (DSR) methodology [4]. The AOCMM integrates principles of adaptability, machine intelligence (MI), and continuous improvement to provide a systematic framework for assessing and enhancing the cybersecurity resilience of CNI organizations. The model's primary contribution is a unified, real-time measurement instrument that facilitates a nationwide or sectoral perspective for comparing maturity levels, thereby guiding optimal cybersecurity investment and policy decisions.

Keywords: Cybersecurity threats, Critical National Infrastructure (CNI), cybersecurity maturity models, adaptability, machine intelligence (MI).

1. Introduction

1.1 Background to the Study

The increasing global reliance on digital systems has made CNI a prime target for sophisticated cyber adversaries [1]. Many organisations grapple with the contemporary cybersecurity vulnerability landscape [21], and cyberattacks are typically known for exploiting the weak points of cyberspace assets, which are inherent vulnerabilities [22]. These vulnerabilities can arise from various factors, such as inadequate security protocols, outdated software, or human errors [23]. As a result, cyberattacks can occur when a malicious party exploits such vulnerability opportunities or when a user unknowingly creates an unintended opening for the attacker to strike [24]. It is essential to address the vulnerabilities present in evolving landscapes to ensure security, safety, and improve the benefits of cyber activities.

Thus, cybersecurity requires intensified research to explore a range of risks that are often overlooked but should receive due attention from individuals, organisations, and governments [25]. Doing so can create a more secure, safe, and resilient cyber environment that can support national security and the digital economy. Organisations need to understand the factors that contribute to these risks

to manage cybersecurity risks effectively [23]. Therefore, having a clear view of the cybersecurity risk landscape is imperative for organisations to apply risk management principles and safeguard their assets and resources against potential cyber threats [21].

1.2 Adaptive Cybersecurity

Nowadays, cybersecurity has become a crucial part of any organisation's operation. Organisations need to adopt a proactive approach towards cybersecurity rather than a reactive one to ensure better protection and resilience against current and evolving threats. They must devise effective adaptive strategies to help them achieve cybersecurity maturity. Consequently, organisations must understand the vulnerability, threat, and risk landscapes by adaptively using cybersecurity maturity models to mitigate current and evolving threats.

In this research, we develop an adaptive cybersecurity maturity model that will equip organisations to protect critical digital assets and resources. The idea is to construct a model that can help organisations assess their degree of cybersecurity maturity, ranging from low to high levels of abstraction. By doing so, organisations would attempt to understand the evolving threat landscape caused by inherent vulnerabilities [26] and how to address them. According to Thycotic (2017), cyber threats cannot be eradicated, implying that cybersecurity's importance lies in mitigating and reducing the impact of these threats [27].

1.3 Cybersecurity Maturity

According to Dube and Mohanty (2020) and Mbanaso and Koleoso (2020), increasing connectivity and advances in cyber technologies increase an organisation's points of potential vulnerability, collectively known as its 'attack surface' [28] [21]. The attack surface has increased significantly due to the proliferation of technologies related to social, mobility, analytics, and cloud (SMAC), the internet of things (IoTs) and the operational technology (OT) used by industrial control systems (ICS).

Cyberattacks occur every second, impacting individuals, businesses, and governments worldwide, and current trends indicate that malicious activities show no signs of slowing down globally [29]. Malicious parties persist in exploiting existing and emerging vulnerabilities [30] and devising new methods to evade cybersecurity measures [31]. Although there are challenges to face, cyberspace's potential to positively impact society is substantial and promising. Implementing cybersecurity regulatory frameworks has set a high standard for organisations to develop effective cybersecurity measures to prevent hostile entities from abusing or exploiting digital assets and resources [24].

Traditional, static maturity models, such as early iterations of the Capability Maturity Model Integration (CMMI) [5], are proving insufficient to manage the dynamic nature of cyber risk [2]. This research addresses the critical need for an adaptive and intelligent mechanism to assess and improve organizational cybersecurity posture. The AOCMM is proposed as a solution, moving beyond descriptive maturity assessment to prescriptive, intelligence-driven resilience enhancement. The model is specifically tailored to the high-stakes environment of CNI, where a cyber incident can have catastrophic national consequences, demanding a shift from compliance-based security to resilience engineering [6].

2. Theoretical Foundation and Related Work

The AOCMM is grounded in a synthesis of established cybersecurity and organizational frameworks, extending their utility through the integration of adaptive intelligence.

2.1. Foundational Maturity Models

The model builds upon the strengths of three primary frameworks:

a) NIST Cybersecurity Framework (CSF): Provides the core functions (Identify, Protect, Detect, Respond, Recover) that define the scope of cybersecurity activities [7].

b) Cybersecurity Capability Maturity Model (C2M2): Offers a comprehensive structure for

evaluating cybersecurity capabilities across various domains, often used in the energy sector [8].

c) NICE Workforce Framework for Cybersecurity: Provides a standardized taxonomy for defining the knowledge, skills, and abilities (KSAs) required for the "People" component of the AOCMM [9].

2.2. Gaps in Existing Models and the Need for Adaptability

While foundational models are essential, they exhibit three critical gaps that the AOCMM is designed to address [10]:

i. Lack of Adaptability: Traditional models are often static, requiring manual updates to reflect new threats. The AOCMM introduces a mechanism for the model itself to evolve in response to new threats and organizational changes.

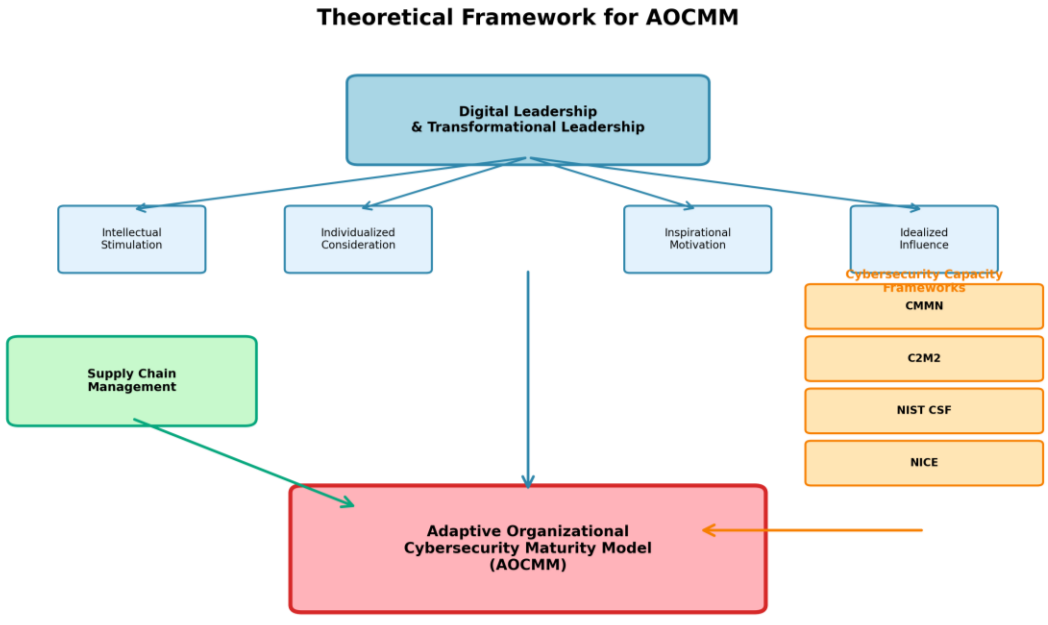
ii. Limited Machine Intelligence Integration: Existing models rarely leverage MI for continuous data curation, real-time assessment, and predictive analytics, which is crucial for modern threat landscapes [11].

iii. Incomplete Capacity and Capability Integration: Many models focus heavily on either technical controls (capability) or governance (capacity). The AOCMM provides a holistic view that equally weighs organizational capacity (e.g., governance, technology) and human capability (e.g., workforce skills, leadership).

2.3. Theoretical Framework

Digital leadership is rooted in transformation, motivating organisational advancements that lead to optimal productivity, efficiency, and profitability [32]. Transformational leaders possess a clear vision, passion, and inspirational qualities. Digital leadership is guided by four principles: intellectual stimulation, individualised consideration, inspirational motivation, and idealised influence [33]. Effective supply chain management involves coordinating relationships with suppliers and partners [34]. Cybersecurity capacity is crucial, with frameworks like CMMN [35], C2M2 [8], NIST's Cybersecurity Framework [36], and the NICE Framework [37] guiding assessing and enhancing cybersecurity capabilities.

Figure 1: Theoretical Framework



These maturity models are widely used worldwide to measure an entity's progress. However, in terms of measuring the organisation's cybersecurity capacity, current models lack an in-depth approach that characterises the notion of capacity in the ever-evolving cyber threat landscape. Notably, the issue of the workforce's knowledge and skills is missing in most models, as well as in the supply chain threat landscape.

3. Design Science Research Methodology

The AOCMM was constructed using the Design Science Research (DSR) paradigm, which is focused on the creation of an innovative and useful artifact to solve a practical problem [4]. The methodology followed the widely accepted six-step process proposed by Peffers et al. [12]:

DSR Phase	AOCMM Implementation	Contribution to Knowledge
1. Problem Identification & Motivation	Recognizing the inadequacy of static CMMs for the dynamic CNI context.	Justification for the research and the need for a new artifact.
2. Define Objectives for a Solution	Defining the need for an adaptive, MI-integrated, and holistic maturity model capable of providing real-time, sectoral-level insights.	Formal specification of the AOCMM's required functionality.
3. Design and Development	Conceptualizing the AOCMM structure, its five core components, and the MI feedback loop.	The AOCMM artifact itself (model, constructs, and metrics).
4. Demonstration	Developing a Python-based proof-of-concept software tool to operationalize the model.	Demonstration of the artifact's feasibility and utility in a simulated environment.
5. Evaluation	Assessing the model and artifact through expert validation and empirical testing (e.g., survey-based evaluation).	Confirmation of the artifact's utility, quality, and academic rigor.
6. Communication	Publication of the model and its implementation (this paper and its companion).	Dissemination of the knowledge to the academic and practitioner communities.

3.1. Research Methodology

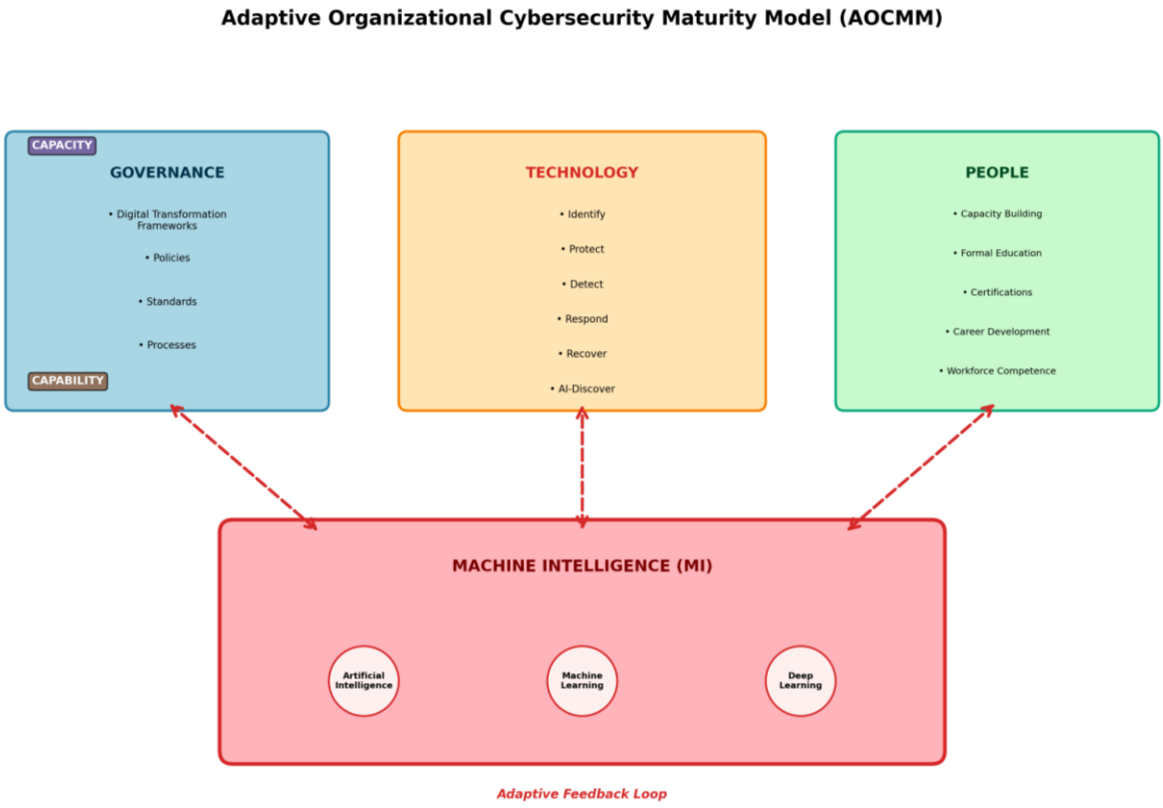
In addition to the DSR strategy, a mixed-methods approach is adopted, as the problem under study is dynamic and requires a pragmatic setting. The Mixed-Methods paradigm combines qualitative and quantitative methods to collect and analyse data,

gaining a deeper insight into the research problem and enriching the design and implementation process. Specifically, the qualitative approach is applied to the Requirement Engineering phase of the artefact conceptualisation, while the quantitative approach is used during Requirement Specification Analysis.

4. The Adaptive Organizational Cybersecurity Maturity Model (AOCMM)

The AOCMM is a multi-dimensional framework structured around five core components, which collectively determine the overall organizational cybersecurity maturity. This holistic approach ensures that maturity is not solely measured by technology but also by the human and process elements that drive resilience [13]. The AOCMM Framework is a theoretical model for measuring the maturity level of organisations in terms of the capacity and capability of the People, Governance and Technological components of the organisation, with the unique feature of being flexible to accommodate future changes in cyberspace. The model can therefore receive feedback and can be constantly tweaked based on future threats to organisations, becoming adaptive in the sense that it can constantly be fine-tuned to suit distinct future situations.

Figure 3: Conceptualised Adaptive Organisational Cybersecurity Maturity (AOCMM) Framework



4.1. AOCMM Core Components

The five components are designed to provide a comprehensive assessment across the entire organization:

Component	Description	Maturity Focus
Capacity	The organizational resources, structure, and processes available to manage cybersecurity, including budgetary allocation and strategic planning.	Resource Allocation, Strategic Planning, Budgetary Support, Policy Frameworks [14].
Capability	The ability of the organization to execute specific cybersecurity functions (e.g., Identify, Protect, Detect, Respond, Recover) as defined by frameworks like NIST CSF.	Functional Effectiveness, Operational Efficiency, Incident Response Readiness, Threat Hunting [7].
Governance	The policies, standards, and leadership commitment that direct and control the organization's cybersecurity efforts, including risk management and regulatory compliance.	Policy Compliance, Risk Management, Executive Oversight, Regulatory Adherence [15].
Technology	The deployment, configuration, and maintenance of security hardware and software solutions, including network security and access control systems.	Tool Efficacy, System Architecture, Security Control Implementation, Zero Trust Principles [16].
People	The knowledge, skills, and awareness of the workforce, including leadership and technical staff, aligning with frameworks like NICE.	Workforce Competency, Security Culture, Training Effectiveness, Human Factor Risk [9].

4.1.1. Governance

Cybersecurity governance encompasses an organisation's framework and processes for managing its cybersecurity risks effectively. This includes the policies, procedures, roles, responsibilities, and oversight mechanisms that guide how the organisation protects its information assets and responds to potential security threats. It involves establishing an organisation's cybersecurity risk management strategy, expectations, and policies that are communicated and monitored effectively. The Governance function provides essential outcomes that guide an organisation in achieving and prioritising the results of its cybersecurity strategy, aligning with its mission and stakeholder expectations. Governance activities are vital for

integrating cybersecurity into the organisation's broader enterprise risk management (ERM) strategy. This governance framework involves understanding the organisational cybersecurity context and managing cybersecurity supply chain risks. Establishing a framework for strategic alignment between ICT security initiatives and overarching business objectives facilitates more informed decision-making regarding the allocation of resources. Effective governance promotes regulatory compliance, thereby mitigating the risk of penalties associated with non-compliance with laws and regulations about data protection and security standards. Additionally, it fosters increased trust among customers and stakeholders by demonstrating a commitment to data protection and ensuring transparency throughout the organisation.

4.1.2. Technology

In this context, "technology" encompasses the cybersecurity infrastructure, tools, and equipment to protect the operational framework from cyber threats and attacks. These elements are integral to establishing a robust defence mechanism to ensure integrity, confidentiality, availability, authenticity, non-repudiation and trust of vital cyber systems in the face of evolving cyber risks. Conversely, capacity can be understood as a function of the foundational infrastructure, equipment, and tools established for cybersecurity defence. In contrast, the capability is determined by effectively applying these components to achieve the desired outcomes. To evaluate an organisation's technological readiness or level of preparedness, we construct our metrics from the five pillars of the NIST Cybersecurity Framework [7].

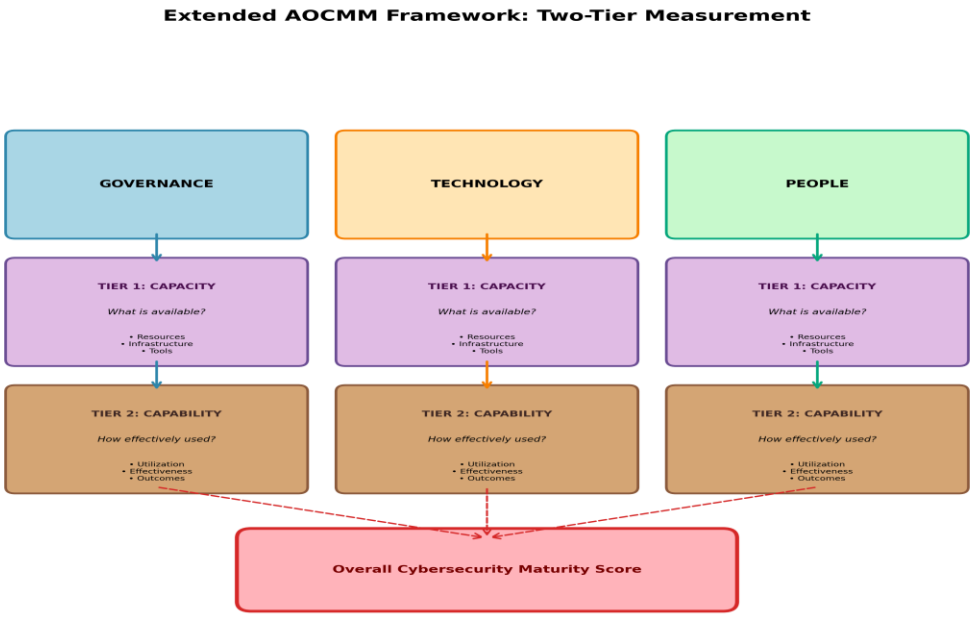
4.1.3. People

The 'People' element of the AOCMM framework refers to the human factors that are critical to an organisation's cybersecurity posture. It encompasses the knowledge, skills, abilities, and awareness of the entire workforce, from the board of directors to the frontline staff. This component recognises that even the most advanced technology and well-defined policies can be undermined by human error or a lack of security consciousness. Therefore, it is essential to cultivate a strong cybersecurity culture where every member of the organisation understands their role in protecting digital assets and is equipped with the necessary training and resources to do so effectively. The NICE Workforce Framework for Cybersecurity [9] provides a standardized taxonomy for defining the knowledge, skills, and abilities (KSAs) required for this component.

4.1.4. Capacity and Capability

Capability denotes the proficient utilisation of resources (capacity) to achieve designated outcomes. This concept encompasses the strategies and processes identified and implemented to transform available resources into practical results, emphasising the importance of resource management and outcome attainment in various contexts. Mere capacity is inadequate; the provision of tools, resources, and training serves only as a foundational element for achieving a mature state of cybersecurity. Capacity implies the extent to which an organisation acquires the necessary tools, technology, and processes to fulfil its operational requirements. In contrast, capability pertains to the effective and efficient utilisation of these resources in executing tasks according to established norms. Capacity assessments evaluate the availability of relevant policies, standards, or frameworks within the organisation's governance structure. At the same time, capability evaluations focus on the effectiveness of these policies in addressing and mitigating cyber threats.

Figure 5: Extended AOCMM Framework showing Two-Tier Measurement



4.2. The Adaptive Mechanism: Machine Intelligence Integration

The Adaptive element is the key differentiator of the AOCMM. It is realized through the continuous feedback loop provided by the integrated Machine Intelligence (MI) Model [11]. As assessment data is collected from CNI entities, the MI component performs the following functions:

i. Data Curation: Aggregates and standardizes assessment data, organizational context, and post-assessment incident reports into a unified dataset.

ii. Threat Correlation: Uses machine learning algorithms (e.g., Bayesian networks or regression models) to correlate specific control measure scores with actual security outcomes (e.g., successful defense against a new threat vector).

iii. Dynamic Weighting: Dynamically refines the weighting and metrics of the five core components and their sub-elements based on the MI model's learning. This ensures the model prioritizes investment in controls that are demonstrably most effective against the current and emerging threat landscape, ensuring continuous relevance [17].

4.3. Cybersecurity Maturity Quadrants (CMQs)

To provide a practical assessment framework, the AOCMM introduces four Cybersecurity Maturity Quadrants (CMQs) that illustrate varying levels of organisational preparedness concerning risk and readiness. These quadrants are derived from the intersection of capacity (resource availability) and capability (resource utilization effectiveness), creating a 2x2 matrix that enables organizations to quickly identify their current maturity position and prioritize improvement efforts.

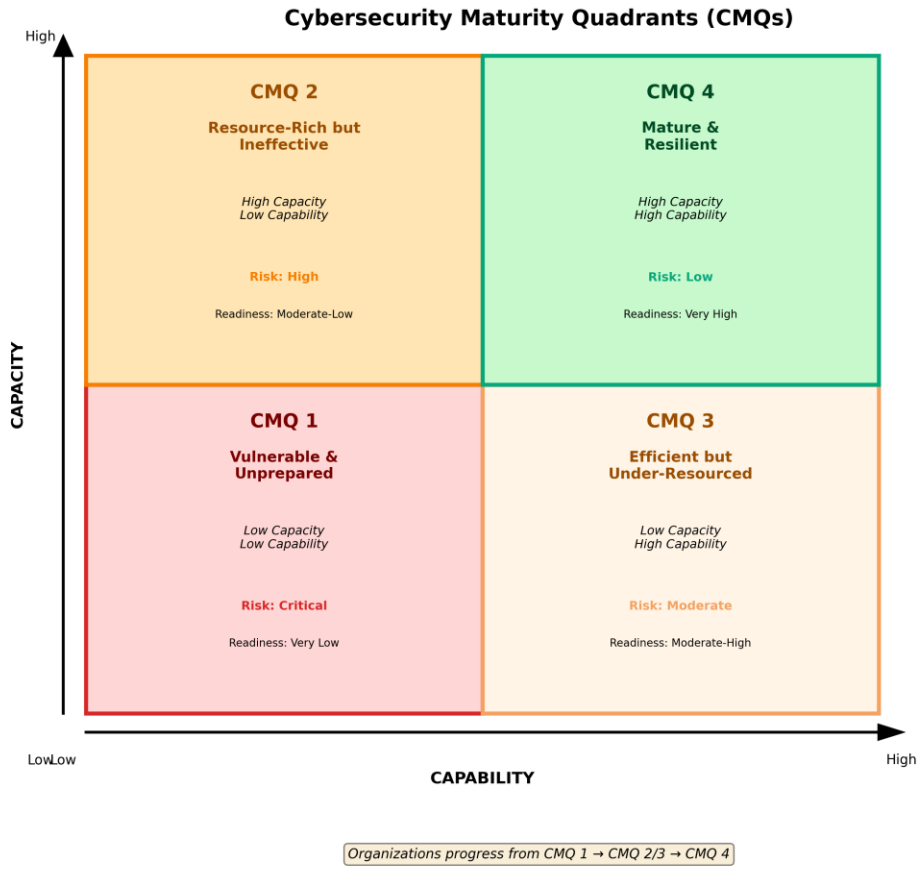


Figure 6: Cybersecurity Maturity Quadrants (CMQ) Matrix

CMQ 1: Vulnerable & Unprepared (Low Capacity, Low Capability)

Organizations in this quadrant face the highest risk exposure due to minimal cybersecurity resources and poor execution of security functions. These organizations typically operate reactively, addressing threats only after incidents occur. Immediate investment in foundational infrastructure, governance frameworks, and workforce development is critical.

CMQ 2: Resource-Rich but Ineffective (High Capacity, Low Capability)

Despite significant investments in cybersecurity tools and infrastructure, organizations in this quadrant struggle with effective implementation and utilization. This often results from a lack of skilled personnel, inefficient processes, or a compliance-focused rather than resilience-focused approach. Priority should be given to capability development through training, process optimization, and security culture enhancement.

CMQ 3: Efficient but Under-Resourced (Low Capacity, High Capability)

Organizations in this quadrant demonstrate high effectiveness with limited resources, often due to a highly skilled workforce and optimized processes. However, resource constraints may limit scalability and create sustainability challenges. Strategic investment in infrastructure and automation can help these organizations scale their capabilities while maintaining efficiency.

CMQ 4: Mature & Resilient (High Capacity, High Capability)

Organizations in this quadrant represent the target state, with comprehensive resources and highly effective utilization. They demonstrate proactive threat management, continuous improvement, and adaptive capabilities. These organizations should focus on maintaining their posture, addressing emerging threats, and contributing to the broader cybersecurity ecosystem through knowledge sharing and innovation.

5. Application to Critical National Infrastructure (CNI)

The AOCMM is specifically designed for CNI, offering a sectoral measurement instrument that addresses the unique challenges of national-level cybersecurity [18]. This allows for:

a) Real-Time Comparison: Benchmarking the maturity of individual CNI entities against national or sectoral averages, facilitating peer-to-peer learning and compliance monitoring. This is a significant improvement over annual, static audits.

b) Targeted Investment: Providing data-driven insights to policymakers for optimal allocation of national cybersecurity resources based on empirically identified weaknesses and MI-driven risk prioritization [19].

c) Unified Perspective: Establishing a common language and standard for cybersecurity maturity across diverse CNI sectors (e.g., energy, finance, telecommunications), which is vital for national resilience and coordinated defense strategies [20].

6. Conclusion

The AOCMM represents a significant advancement in cybersecurity maturity modeling. By employing a rigorous DSR approach and embedding adaptability and intelligence at its core, it provides CNI organizations with a robust, dynamic, and prescriptive framework for enhancing resilience. This model shifts the focus from static compliance to dynamic, intelligence-driven risk management, a necessity for protecting national critical assets. The framework's adaptive nature allows it to evolve and accommodate future cyber threats, regulatory changes, and technological advancements. Future work will focus on the large-scale deployment and continuous refinement of the MI component to further validate the model's adaptive capabilities and its long-term impact on national cybersecurity posture, as well as the development of component-wise metrics for capacity and capability cybersecurity maturity measurement and proof-of-concept artefact development.

References

[1] The Global Cybersecurity Forum. (2023). The Future of Cyber Resilience Report.

[2] U.S. Department of Energy (DOE). (2022). Cybersecurity Capability Maturity Model (C2M2).

[3] National Institute of Standards and Technology (NIST). (2024). Cybersecurity Framework (CSF).

[4] Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3), 45-77.

[5] Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). Capability Maturity Model for Software.

[6] Linkov, I., et al. (2018). Resilience Engineering: A New Paradigm for Cyber-Physical Systems.

[7] National Institute of Standards and Technology (NIST). (2024). Cybersecurity Framework (CSF).

[8] U.S. Department of Energy (DOE). (2022). Cybersecurity Capability Maturity Model (C2M2).

[9] National Institute of Standards and Technology (NIST). (2020). NICE Workforce Framework for Cybersecurity.

[10] Papachristofis, K., et al. (2024). Comparative Evaluation of Cybersecurity Maturity Models and Frameworks.

[11] Mohamed, N., et al. (2025). Artificial intelligence and machine learning in cybersecurity.

[12] Peffers, K., et al. (2007). A design science research methodology for information systems research.

[13] Mbanaso, U. M., et al. (2020). Cybersecurity Supply Chain Vulnerability.

[14] Gampel, A., & Eveleigh, T. (2025). Model-Based Systems Engineering Cybersecurity Risk Assessment for Industrial Control Systems Leveraging NIST Risk Management Framework Methodology.

[15] Franco, V. R. (2024). Three Steps Toward a Digital Governance Framework (DGF).

[16] Rose, S., et al. (2020). Zero Trust Architecture.

[17] Oragwu, U. (2025). A Machine Learning Approach for Detecting Cybersecurity Vulnerabilities.

[18] Cavelty, M. D. (2013). Cyber-security and the politics of insecurity.

[19] Sulaiman, R. B., & Khraisat, A. (2025). Metaheuristic-Driven Feature Selection with SVM and KNN for Robust DDoS Attack Detection.

[20] Makinde, J. O., et al. (2020). Cybersecurity Controls and Measures.

[21] Mbanaso, U., & Koleoso, R. A. (2020). An Investigation of Cybersecurity Vulnerability Landscape.

[22] Mbanaso, U. M., Kulugh, V. E., & Makinde, J. A. (2019). Characterisation of Critical Infrastructure Organisation in Nigeria.

[23] Wang, B. (2022). 7 Most Common Types of Cyber Vulnerabilities.

[24] King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment. Frontiers in Psychology, 9(39).

[25] Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, Challenges and Future Directions. Cyber Security and Applications, 2(2), 100031.

[26] Subashini, K. K. P, & Fernando, S. (2018). Survey on cyber security measures and their applicability in digital business ecosystem.

[27] Thycotic. (2017). The 2017 State of CyberSecurity Metrics Annual Report.

[28] Dube, D. P., & Mohanty, R. P. (2020). Towards development of a cyber security capability maturity model. International Journal of Business Information Systems, 34(1), 104.

[29] Kulugh, V. E., Mbanaso, U. M., & Chukwudebe, G. (2022). Cybersecurity Resilience Maturity Assessment Model for Critical National Information Infrastructure. SN Computer Science, 3(3).

[30] Mbanaso, U., & Dandaura, E. (2015). The Cyberspace: Redefining A New World. IOSR Journal of Computer Engineering (IOSR-JCE), 17(3), 17–24.

[31] Desouza, K. C., Ahmad, A., Naseer, H., & Sharma, M. (2020). Weaponizing information systems for political disruption: The Actor, Lever, Effects, and Response Taxonomy (ALERT). Computers & Security, 88, 101606.

[32] Allen, G. P., Moore, W. M., Moser, L. R., Neill, K. K., Sambamoorthi, U., & Bell, H. S. (2016). The Role of Servant Leadership and Transformational Leadership in Academic Pharmacy. American Journal of Pharmaceutical Education, 80(7), 113.

[33] Ratajczak, S. (2022). Digital leadership at universities - a systematic literature review. Forum Scientiae Oeconomia, 10(4), 133–150.

[34] Van der Vorst, J. (2004). Supply Chain Management: Theory and Practices.

[35] Saïd Business School. (2017). Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition.

[36] Quinn, S., Pascoe, C., Barrett, M., Scarfone, K., & Witte, G. (2024). NIST Cybersecurity Framework 2.0: Quick-Start Guide for Using the CSF Tiers.

[37] NICCS. (2023). Workforce Framework for Cybersecurity (NICE Framework).