https://dx.doi.org/10.4314/dujopas.v11i1b.9
ISSN (Print): 2476-8316
ISSN (Online): 2635-3490
Dutse Journal of Pure and Applied Sciences (DUJOPAS), *Vol. 11 No. 1b March 2025*

Theoretical Framework of Cybersecurity Resilience Maturity Assessment Model for Critical Information Infrastructure

Victor Emmanuel Kulugh[1], Ageebee Silas Faki[2,] and Egena Onu[3]

[1, 3]Department of Cybersecurity,
Bingham University,
Karu,
Nigeria.

[2]Department of Cybersecurity,
Baze University,
Abuja,
Nigeria.

Email: victor.kulugh@binghamuni.edu.ng

Abstract

Modern Societies depend heavily on Critical infrastructures (CIs) to thrive. The CI in turn is driven by critical information infrastructures (CIIs) which is a combination of information technology (IT) and operations technology (OT). However, the CIs are underpinned by the CIIs, thus, they (CIs) inherit the vulnerabilities of the CIIs and share the same threats as the CIIs. Failure of the CIIs driving the CIs will potentially lead to catastrophic consequences arising from cascaded, escalating and common cause effects against other dependent/interdependent CIs/CIIs. Consequently, the CIIs should be resilient against cyberattacks. To enhance the cybersecurity resilience of CIIs, maturity models (MM) are developed to measure their cybersecurity resilience, determine resilience gaps and proactively close these gaps for improved resilience. However, existing MMs and frameworks for this purpose lack theoretical foundations or at least their underlying theories are not transparent. This makes the models either too generic or too industry-specific for adoption in the CII ecosystem. Consequently, this article proposes a theoretical framework for developing cybersecurity resiliency maturity assessments models for CIIs based a combination of the Bruneau Resilience Theory (BRT), Socio-Technical Systems Theory (STST) and Hollings' Ecosystem Theory of Resilience (HETR). While the BRT supports the presentation of an MM that addresses CII resilience quantification from 3 temporal dimensions, namely; pre-event, event management (during-event) and post-event activities; the STST provides the ground for a proportionate combination of controls that measures the ability of CIIs to treat threats of technogenic, anthropogenic and naturogenic origin; lastly, the HETR forms the basis for continuous resilience assessment at defined regular intervals.

Keywords: critical information infrastructures, maturity models, cybersecurity, resilience.

INTRODUCTION

Digital technologies have transformed traditional enterprises into technology dependent organisations for the purpose of removing the barriers of time and location. These barriers formed hindrances to free flow of access to services and products. New business models and

**Author for Correspondence*

industries have also emerged that owe their entire existence to the digital infrastructure. The advantages and opportunities associated with the application of information and communication infrastructure to drive the traditional enterprise and create new ones are endless. In the contemporary society, health-care, commerce, education, banking, social, political engagements, etc are information and communication technology (ICT) driven. The industrial control systems (ICS) that drive physical systems programmatically is a huge area of technology application that the connected society depends on. A combination of all these have created what is today referred to as critical information infrastructure (CII). CII is a combination of information technology (IT) and operations technology (OT) systems to provide modern services, products and functions. There are no generally acceptable definitions of CII, however, they are defined in the context of their applications. For instance, nations define CII in the context of their individual national interests. For instance, (Australian Government, 2010; Mrad, Wiseman, and McLaughlin, 2014; Saeed, *et al*., 2023; USA Patriot Act, 2001). Similarly, organisations define CII based on their goals (ITU) (ITU-T, 2014). However, (Maglaras *et al*., 2018) defined CII as assets that are very important such that their incapacitation, degradation or destruction will potentially have devastating consequences that negatively impact national security, national economy, safety, general wellbeing and shared prosperity of the society. These definitions bring to fore the fact that the notion of criticality is based on the functions and services an asset provides a society and the impacts resulting from the latent consequences that emerge when assets experience failures, disruptions, or degradations that render them unable to deliver those services.

CII have increasingly become important as a consequence of urbanisation, population growth and the demands that services are available 24 hours a day and 7 days a week. These demands have strained traditional organisations and infrastructure beyond their designed capacity (Klaver and Luiijf, 2021; Ryba, 2014). Meeting these growing performance requirements demands that the operating capabilities of the traditional organisations are extended. Thus, accounting for more integration of CII into the core processes of these organisations as the only viable alternative that supports the extension or expansion of organisational capabilities (Sharma, 2017). However, the cyber infrastructure (CII) has ushered in an intricate web of interconnectivity, fostering extensive interconnectedness both within and among contemporary enterprises. Thus, becoming the epicentre of interdependencies and consequently, the cyberquakes of now and the future (Lewis, 2019). The CII that underlies the modern organisation and the society are ladened with vulnerabilities that threats constantly seek to exploit. The interdependencies created through interconnectivity are further expanding the attack surface and the threat vectors proportionately. They (CII) are force multipliers in the propagation of cascaded, escalated and common cause failures in organisations (Rehak *et al*., 2016). Traditional approaches such as critical information infrastructure protection (CIIP) are no longer sufficient to adequately tackle the emerging gamut of challenges threatening to undermine the undisturbed functioning of the organisation. This is as a result of the new and evolving threats and vulnerabilities landscape arising from the integration of CIIs with modern organisations. Thus, Making critical information infrastructures resilience (CIIR) a preferred alternative, (Rod *et al*., 2016).

However, achieving CII resilience requires that organisations firstly develop methodologies and tools that support them to regularly gauge the resilience level and present a clear picture of their current resilience status, identify the gaps in resilience and the sources of these gaps so that they are closed to improve the state of resilience. Maturity models (MM) offer great potentials for the quantification of the resilience maturity of CII. MMs have been found to be effective in the assessment of the maturity of the practices in enterprises, systems and

processes and thus, support organisations to compare current maturity levels against best practices (Aliyu *et al*., 2020, Rios, *et al*., 2023). However, developing MMs that assesses the resilience of CII in organisations depends on how the concept of resilience is operationalised. Operationalising resilience is contingent upon the theoretical definition of the concept. Although, (Tim and Jonas, 2012) argued that the resilience problem is both theoretical and practical; majority of the existing models and frameworks are not based on known theoretical foundation or evidence of the underpinning theories are not transparent (Mettler, 2011; Pereira and Serrano, 2020). For example, notable cybersecurity maturity frameworks and models like the National Institute of Science and Technology (NIST, 2023), Cybersecurity Capability Maturity Model (C2M2) and Cybersecurity Maturity Model Certification (CMMC) etc, have no known theoretical frameworks that underpin their development. Consequently, this paper addresses this gap by proposing theoretical framework that supports the operationalisation of the concept of resilience in a manner that provides a basis for the modelling of the assessment of the resilience of CII and demonstrate how these theories can be adopted to develop measurement metrics for the computation of the resilience maturity of CII in organisations. This work introduces a novel theoretical framework for operationalising the concept of resilience within CII, directly addressing a critical gap in current practices. Unlike existing maturity models and frameworks—which often lack a clear theoretical underpinning or rely on opaque methodologies—this study grounds the assessment of CII resilience in well-established theoretical principles. This approach not only enhances the transparency and replicability of resilience evaluations but also enables the development of precise measurement metrics for quantifying resilience maturity.

Maturity models (MMs) define a structured set of attributes, characteristics, and indicators that represent progression within a specific domain ((Bommareddy *et al*., 2022; Panevski (2023)). These models are developed through consensus among experts and validated with empirical data and iterative recalibration (Caralli *et al*., 2012). They provide organisations, sectors, or nations with standardized tools to measure their current level of maturity, identify weaknesses, and plan for improvements (Pereira and Serrano, 2020). MMs can evaluate various components of an enterprise by comparing diverse units or ranking measurement attributes, and they are often aggregated into indices to assess community performance. Generally, these models consist of standard elements such as model levels, domains, appraisal methods, and improvement roadmaps (Mettler, 2011).

There are three main types of maturity models: progression, capability, and hybrid (Becker et al., 2009). Progression models offer a roadmap for improvement by defining increasingly advanced stages of attributes Babar and Ali (2022), while capability models measure organisational processes and maturity across defined scales, ranging from ad hoc to optimized (Caralli, *et al*., 2012). Hybrid models combine these approaches to express both the degree of achievement and underlying capabilities (Malatj,*et al*., 2019). These types of models have been applied in cybersecurity resilience assessments for Critical Information Infrastructure (CII), allowing organizations to benchmark their resilience against best practices Larsson and Groβe (2023). However, many existing frameworks in this area lack a clear theoretical foundation, which is critical for fully operationalizing and measuring resilience.

Several researchers have proposed cybersecurity resilience models for CII, yet most of these works fall short of providing a robust theoretical basis Abuhasel (2023). For example, some frameworks focused on identifying measurement pillars or used methods like the Fuzzy Analytic Hierarchy Process without thoroughly addressing the foundational concept of resilience Mbanaso, *et al*., (2019). Other studies introduced models specific to particular

domains, such as SCADA systems in power grids or resilience frameworks using artificial intelligence, but they often addressed resilience as isolated issues—such as recovery or prevention—without considering its holistic, temporal, and socio-technical dimensions (Caralli *et al*., 2012; Miron and Muita, 2014; USA Department of Defence [USADoD], 2020). This gap underscores the need for a theoretical framework that can comprehensively support the operationalization and measurement of CII resilience. The remaining sections of the articles are organised as follows: section 2 contains the related works, the methodology is addressed in section 3, the cybersecurity resilience maturity assessment theoretical model (CRMAFM) is presented in section 4 and section 5 concludes the paper.

MATERIALS AND METHODS

Figure 1 presents the methodology framework for developing the theoretical basis for cybersecurity resilience measurement model for CII. Composite indicators are required to build a model that effectively measures the cybersecurity resilience of entities. However, the goal in this article is to ensure that these indicators are theoretically founded.

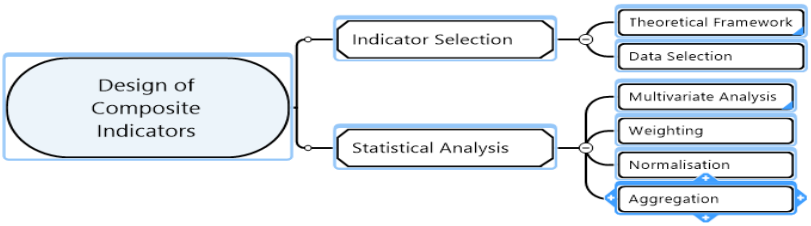

Figure 1: Methodology Framework

Figure 1 depicts a methodology that combines sub-indicators into a meaningful composite indicator under a fit-for-purpose principle. Literature was used to identify theories, provide definition of concepts, determining the sub-groups and determine the selection criteria. The theoretical framework was used to clearly define the areas and the objectives that the composite indicator will measure. The data (indicators or variables) selection follows as it is crucial by the fact that the strengths and weaknesses of composite indicators is derived from the quality of the underlying variables. These variables were selected on the bases of their relevance, analytical soundness and accessibility based on (Organization for Economic Cooperation and Development [OECD], 2008)

Flowing from 'design of composite indicators' and in parallel with 'indicator selection' is the statistical analysis. Thus, Multivariate Analysis (MA) was conducted to investigate the overall structure of the indicators, assess the suitability of the data set and explain the methodological choices such as normalisation, weighting and aggregation. Several methodologies for multivariate analysis including, Principal Component Analysis (PCA), Factor Analysis (FA), Cronbach Alpha, and Cluster Analysis exist. Each with their weaknesses and strengths (Jabareen, 2009; Rocco and Plakhotnik, 2009). However, PCA was adopted because of its ease of use. Weighting was used to show the contributions of indicators at different levels of the model. Normalisation was also done for the purpose ensuring that values of the computations from stayed within the range of 0.00 to 1.00. Conversely, aggregation supported the summation of variables into their composite indicators at the different levels of the model to compute the cybersecurity resilience index.

RESULTS AND DISCUSSION

Figure 2 presents a conceptualisation of the cybersecurity resilience maturity assessment theoretical model made up of the theoretical framework, data selection, normalisation, weighting and aggregation. This is in tandem with the methodology described in section 3.

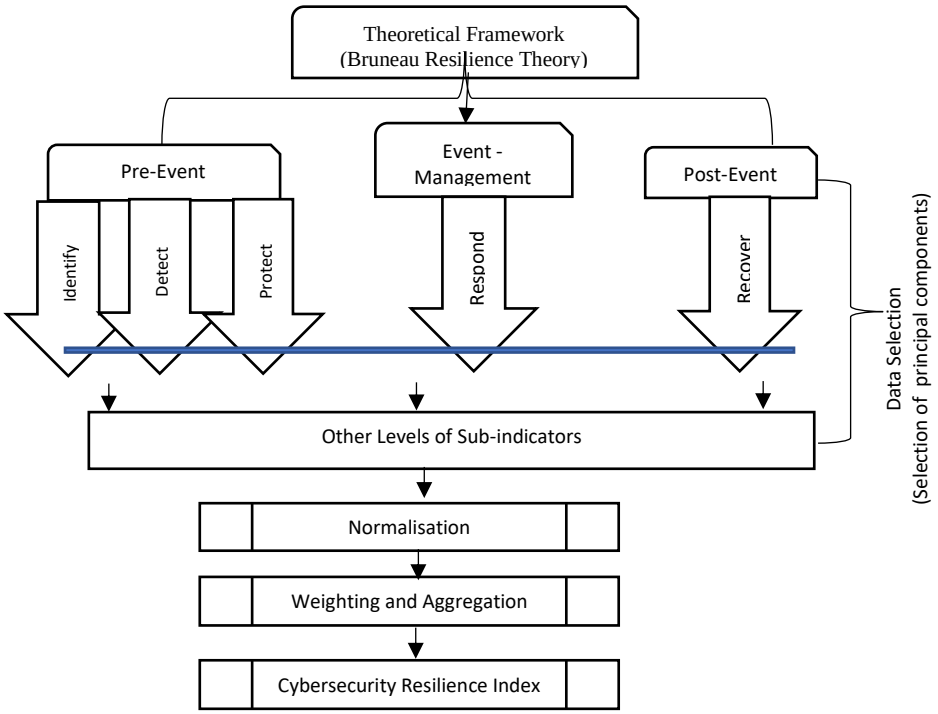

Figure 2: Cybersecurity Resilience Maturity Assessment Theoretical Framework (CRMATF)

Three theories associated with the resilience concept provided the definitions that supported the theoretical framework. These theories formed the basis for data selection (i.e selection of principal components) of the cybersecurity resilience maturity assessment model (CRMAM). The theories and how they support the building of the CRMAM are highlighted as follows:

Bruneau Resilience Theory (BRT)

The BRT defined resilience as the ability of a system to minimise the probability and impact of successful attacks; and decrease the mean time to recovery (MTTR) after attacks (Bruneau *et al*., 2003). Although, BRT was designed for the study of communities' resilience to earthquakes. However, its temporal dimensions show significant promises to address the *cyberquakes* of now and the future. Thus, it was adopted in the theoretical framework of this work. It shows potentials for the quantification or assessment of cybersecurity resilience with respect to its temporal dimensions as presented in the definition, namely: pre-event (before an attack), event management (active phase of an attack) and post-events (post attack) (Bruneau *et al*., 2003). This is referred to as the *Bruneau resilience triangle* with vertexes as pre, during and post attacks. As presented in Figure 2, it proposes the reduction of the likelihood of failures or cyberattacks - (a pre-event activity), minimise the effect of failure – reduction in the magnitude and duration of a disruptive events (an active event phase activity). Reduce the time to recovery (post-event activity). These elements of the BRT that forms part of our theoretical framework are referred to as Resilience Temporal Dimensions (RTD). The BRT is presented in Figure 3.

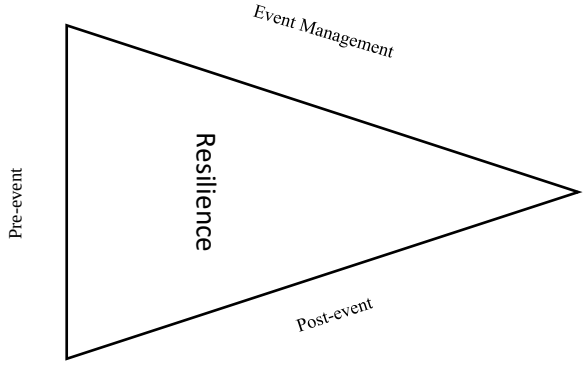

Figure 3: Bruneau Resilience Triangle: Based on (Bruneau *et al*., 2003)

Immediately below the RTD are a set of sub-indicators mapped into each RTD with respect to what each RTD intends to measure. These sub-indicators are derived from the NIST framework (NIST, 2018). They are mapped thus: pre-event (identify, detect and protect); event management (respond) and post-event (recover). Other sub-indicators will be defined under this set until granular measurement is achieved.

Socio-Technical Systems Theory (STST)

Emery and Trist, (1960) propounded the STST to explain a system where humans, machines and the organisational elements intricately interact within the work system. It emphasised the fact that an organisation is made up of a combination of interacting sub-systems. It is a method that seeks to enhance the configuration and correlation between the social and technical dimensions of a system, while considering the systems' environment (Malatj *et al*., 2019; Walker, 2015). Put differently, organisations recruit people with capabilities to perform certain functions; who work towards goals based on processes, apply technology, operate within shared physical or virtual infrastructure and certain cultural assumptions and norms. The STST is presented in Figure 4.

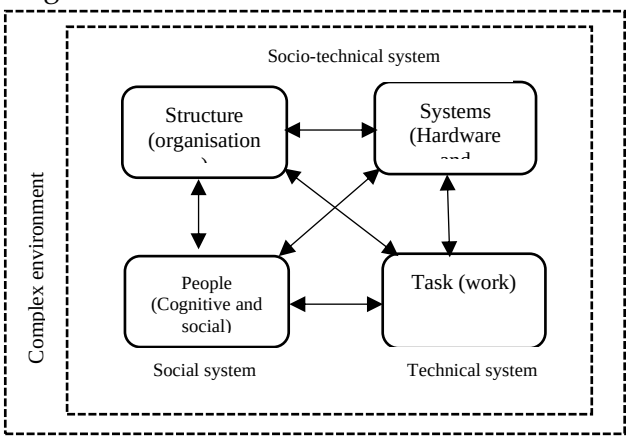

Figure 4: Socio-Technical System (Appelbaum, 1997)

The STST is applied in our theoretical framework to ensure a balance between the cybersecurity controls of people, process and technology. It ensures that upon the selection of indicators, they create a balance in measuring cybersecurity capabilities with respect to all elements that forms the organisation. As illustrated in Figure 4.

Hollings's Ecosystem Theory of Resilience (HETR)

In theory development of resilience, Hollings's Ecosystem Theory of Resilience (HETR) was the first contribution in 1973. This theory was proposed on the bases of observations and states that social-ecological systems can have more than one equilibrium (Holling, 1973). This was contrary to the prevailing understanding at that time, that there was only one state of equilibrium for social-ecological systems that the system will always return after a perturbation. The threat landscape as a key variable of cyber infrastructure resilience that makes up the CII is constantly evolving, thus raising the assumptions that cyber systems may have varying points of resilience equilibrium as different threats, vulnerabilities are uncovered or after cybersecurity incidents have occurred. This reenforces the argument that CII resilience be measured at designated intervals to ascertain the level of resilience and the gaps that may be required to be filled to achieve the targeted level of resilience or even identify new gaps arising in new threats associated with new technologies that may underlie the CII or CI.

Data Normalization

According to (Organization for Economic Cooperation and Development [OECD], 2008) data normalisation should be conducted before weighting an aggregation. Accordingly, this article proposed the use of the *standardisation* data normalisation approach (Peshawa, *et al*., 2014) applied with the formula presented in equation 1:

$$I^{t}_{qm} = \frac{x^{t}_{qm} - x^{t}_{qm} = m}{Q^{t}_{qm} - m} \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Where x^{t}_{qm} = individual indicator, $x^{t}_{qm} - m$ is the average based on the number of indicators and $Q^{t}_{qm} - m$ is the standard deviation across the CIIs. The essence is to ensure that values of computations of the various indicators and sub-indicators are made uniform (i.e maintained between 0.00 – 1.00) to provide uniform values that support comparative analysis among organisation or CIIs and among different cybersecurity resilience indicators within an organisation or CIIs.

Weighting System

Although, there are several approaches to weighting, this article derives the weighting of the principal indicators defined in the theoretical framework as RTD – namely; pre-event, event-management and post-event from a cyber risk-based perspective. Thus, it is proposed that the principal indicator (RTD) with potential to reduce cyber risk the most and with greater number of sub-indicators be allocated more weight.

Table 1:Weighting of Resilience Temporal Dimensions (Kulugh, *et al*., 2022)

#	Principal Indicator (RTD)	Sub-Indicator	Weight
1	Pre-event	Identify	
		Detect	0.55
		Protect	
2	Event-Management	Respond	0.30
3	Post-Event	Recover	0.15
	Total		**1.00**

It is considered that the pre-event RTD has 3 sub-indicators (Table 1) that work to minimise the likelihood of successful cyber-attacks. Thus, from a cyber risk view point, it contributes

more to reducing the potential cyber risk exposure of CIIs by its preventive value. therefore, it is weighted 0.55 (55%), the event-management RTD, though with a single RTD is allocated double the weight 0.30 (30%) of the post-event (which has 0.15 or 15%), (Kulugh *et al*, 2022 and Mbanaso *et al*, 2019). This consequent upon the fact that the event-management RTD plays a crucial role in the event of successful cyberattacks by providing response that reduces the impact and length of the attack. This potentially keeps the system from been degraded beyond levels which they can provide services. The post-event dimension on other hand though very important is remedial, thus weighting 0.15.

Aggregation

We offer an aggregation mechanism in which indicators referred to in Figure 5 as cybersecurity controls at every level (layer in Figure 5) can be aggregated to generate quantitative values that provide insights into the cybersecurity resilience of a CII or organisation at that level. Figure 5 illustrates a six-layered framework showing indicators and sub-indicators. These layers are connected together with respect to the theoretical framework in Figure 2.

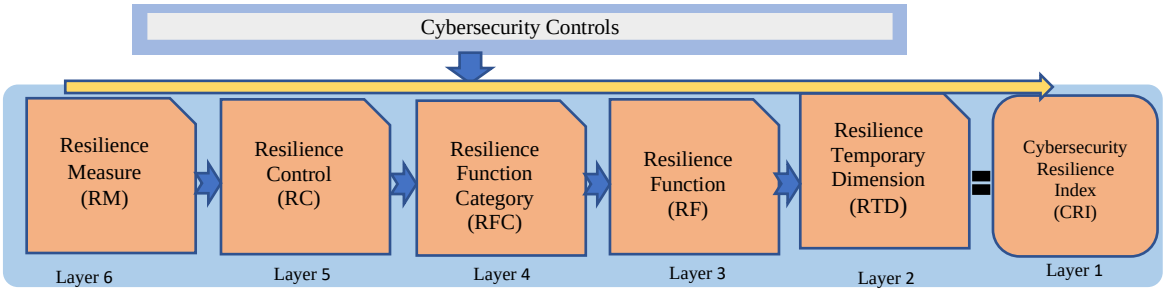

Figure 5: Conceptual Framework for Cybersecurity Resilience Maturity Assessment based on CRMAFT

The elements in layer 6 present the actual measurement of cybersecurity resilience in quantitative terms. The layer 6 elements are aggregated to generate quantitative values of layer 5. Layer 5's values are aggregated to obtain the quantitative result of layer 4. This procedure is iterated till the values of the 3 RTDs are generated. An aggregation of the values of the RTDs gives us the cybersecurity resilience index (CRI) of a CII or organisation.

CONCLUSION

This article created Cybersecurity Resilience Maturity Assessment Theoretical Model (CRMATM) and illustrated how the CRMATM can form the basis for generating composite indicators for cybersecurity resilience maturity assessment of CIIs. It highlighted how the theoretical definitions of the concept of resilience can be applied to generate key indicators of the cybersecurity resilience maturity measurement model. Thus, this conceptualisation can be applied by other researchers as first step in evolving MMs for cybersecurity resilience maturity measurement. The article demonstrates how several sub-indicators can be created flowing from the theoretical framework and how a blend of theories can support the process of creating a cybersecurity resilience maturity index that robustly covers the triads of people, process and technology while also addressing the environmental context. It further showed how the concepts of data normalisation, weighting and aggregation can be applied to augment the computational capabilities of the MM. However, this is a conceptual model that will be implemented as a software and tested in future research.

REFERENCES

Abuhasel, K. A. (2023). Linear Probabilistic Resilience Model for Securing Critical Infrastructure in Industry 5.0. *IEEE Access*. 10.1109/ACCESS.2023.3300650, 4(3), 12-18.

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., and Janicke, H. (2020). A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom. *Applied Sciences: MDPI*. https://doi.org/10.3390/app10103660, 3(1), 18-31.

Australian Government. (2010). Critical Infrastructure Resilience Strategy. In *Report* (Issue September 2001). papers2://publication/uuid/C8ECF2E8-3ED2-4881-86E2-39F8F0581282%5Cnhttp://www.tisn.gov.au/documents/australian+government+s+critical+infrastructure+resilience+strategy.pdf, 3(1), 78-86

Babar, A. H. K. and Ali, Y. (2022). Augmentation of Resilience in Critical Infrastructure: Developing Countries a Case in Point. *Technology in Society*. https://doi.org/10.1016/j.techsoc.2021.101809, 4(1), 99-108.

Bade, M., and Mohammed, I. (2019). Cyber Security Capability Maturity Model for Critical Information Technology Infrastructure Among Nigeria Financial Organizations. *International Journal of Current Research,11(6), 4796-4799,* DOI: https://doi.org/10.24941/ijcr.35585.06.2019

Baumgartner, J., Hood, J., Korcher, T., Steinberg, B., and Lagraffe, D. (2019). Cybersecurity Capability Maturity Model (C2M2) Version 2.0. *U.S. Department of Energy*. Retrieved from https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021_508.pdf, 5(1), 56-68

Becker, J., Knackstedt, R., and Pöppelbuß, J. (2009). Developing Maturity Models for IT Management – A Procedure Model and its Application. *Entwicklung von Reifegradmodellen Für Das IT-Management – Vorgehensmodell Und Praktische Anwendung. WIRTSCHAFTSINFORMATIK.*, Ralf Knackstedt. https://doi.org/10.1007/s12599-009-0044-5, 6(3), 41-56

Bommareddy, S., Gilby, B., Khan, M., Chiu, I., Pantelli, M., van de Lindt, J. W., Wells, L. I., Amir, Y., & Babay, A. (2022). Data-Centric Analysis of Compound Threats to Critical Infrastructure Control Systems. *15th International Conference on Cyber Risk Assessment of UAVs*, 15(1), 204–212

Bruneau, M., Eeri, M., Chang, S. E., Eeri, M., Ronald, T., Eeri, M., Lee, G. C., Eeri, M., Rourke, T. D. O., Eeri, M., Reinhorn, A. M., Eeri, M., Shinozuka, M., Eeri, M., Wallace, W. A., and Winterfeldt, D. Von. (2003). A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthquake Spectra 19*(4), 733–752. https://doi.org/10.1193/1.1623497

Caralli, R., Knight, M., and Montgomery, A. (2012). Maturity Models 101: A Primer for Applying Maturity Models to Smart Grid Security, Resilience, and Interoperability. *Carnegie Mellon University. 2012_019_001_58920, 15(2), 19-27*

Emery, F. E., and Trist, I. E. (1960). Socio-Technical Systems. In C. W. Churchman and M. Verhulst (Eds.), *Management Science: Models and Techniques* (First, pp. 83–97). Pegamon.

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, *4*(1), 1–24. https://doi.org/10.1146/annurev.es.04.110173.000245

ITU-T. (2014). Requirements for Network Resilience and Recovery (Vol. 1.0). FG-DR&NRR http://handle.itu.int/11.1002/pub/80ad53fe-en, 1(1).

Jabareen, Y. (2009). Building a Conceptual Framework: Philosophy, Definitions, and Procedure. In *International Journal of Qualitative Methods* 8(4), 101-115.

Klaver, M., and Luiijf, E. (2021). Analyzing the Cyber Risk in Critical Infrastructures. In *Issues on Risk Analysis for Critical Infrastructure Protection*. IntechOpen. https://doi.org/10.5772/intechopen.94917, 9(3), 97-108.

Larsson, A., & Groβe, C. (2023). Data Use and Data Needs in Critical Infrastructure Risk Analysis. *Journal of Risk Research*. https://doi.org/10.1080/13669877.2023.2181858, 12(2), 77-85.

Lewis, L. P. (2019). Critical Infrastructure Interdependency Analysis: Operationalising Resilience Strategies. *Contributing Paper to GAR 2019. https://www.undrr.org/quick/11783, 7(1), 1-11.*

Maglaras, L. A., Kim, K. H., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., Maglaras, A., and Cruz, T. J. (2018). Cyber security of critical infrastructures 4(1), 42–45). *Korean Institute of Communications Information Sciences*. https://doi.org/10.1016/j.icte.2018.02.001

Malatj, M., Solms, S. Von, and Marnewick, A. (2019). Socio-Technical Systems Cybersecurity Framework, *Information and Computer Security*. https://doi.org/https://doi.org/10.1108/ICS-03-3(1), 2018-0031

Mbanaso, U. M., Abrahams, L., & Apene, O. Z. (2019). Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework. *The African Journal of Information and Communication*, 23(23), 1–26. https://doi.org/10.17159/2077-7213/2019/n23a2

Mettler, T. (2011). Maturity Assessment Models: A Design Science Research Approach. *International Journal of Society Systems Science* 1(2), 81-98 10.1504/IJSSS.2011.038934

Miron, W., and Muita, K. (2014). Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure. *Technology Innovation Management Review* 4(10), 33-39 10.22215/timreview/837

Mrad, N., Wiseman, E., and McLaughlin, T. (2014). Critical Infrastructure Protection and Resilience Literature Survey: State of the Art. *National Research Council, Canada*. https://cradpdf.drdc-rddc.gc.ca/PDFS/unc200/p801837_A1b.pdf, 7(4), 15-24.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. https://doi.org/10.6028/NIST.CSWP.04162018, NIST Publiction 800-30

Office of the National Security Adviser [ONSA] (2021). National cybersecurity policy and strategy. *Federal Republic of Nigeria.* http://ctc.gov.ng/wp-content/uploads/2021/02/NATIONAL-CYBERSECURITY-POLICY-AND-STRATEGY-2021_E-COPY_24223825.pdf

Organization for Economic Cooperation and Development (OECD). (2008). Handbook on Construction Composite Indicators: Methodology and User Guide. *JRC European Commission*. https://www.oecd.org/sdd/42495745.pdf

Panevski, V. (2023). Organizational Resilience and Critical Infrastructure Security Systems. *International Scientific Journal "Security & Future"*. 7(1), 3-5 WEB ISSN 2535-082X; PRINT ISSN 2535-0668

Pereira, R., and Serrano, J. (2020). A Review of Methods Used on IT Maturity Models Development: A Systematic Literature Review and a Critical Analysis. *Journal of Information Technology*, *20*(1), 1–18. https://doi.org/https://doi.org/10.1177/026839621988687

Peshawa, J. Ali, M. Faraj, R. H. (2014). Data Normalization and Standardization: A Technical Report*Machine Learning Technical Reports*, 1(1), 1-6 10.13140/RG.2.2.28948.04489

Rea-Guaman, A.M., Feliu, T. S., Calvo-Manzano, J. A., Garcia, I.D.S. (2017). Comparative Study of Cybersecurity Capability Maturity Models. *International Conference on*

Software Process Improvement and Capability Determination. 10.1007/978-3-319-67383-7_8, 7(3), 212-223

Rehak, D., Markuci, J., Hromada, M., and Barcova, K. (2016). Quantitative Evaluation of the Synergistic Effects of Failures in a Critical Infrastructure System. *International Journal of Critical Infrastructure Protection*, *142)*, 3–17. https://doi.org/10.1016/j.ijcip.2016.06.002

Rios, G., Iturbe, E., Rego, A., Ferry, N., Tigli, J., Lavirotte, S., Rocher, G., Nguyen, P., Song, H., Dautov, R., Mallouli, W., & Cavalli, A. R. (2023). The DYNABIC approach to resilience of critical infrastructures. ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security August 2023Article 136(12), 1–8. https://doi.org/10.1145/3600160.3605055

Rocco, S. T., and Plakhotnik, S. M. (2009). Literature Reviews, Conceptual Frameworks, and Theoretical Frameworks: Terms, Functions, nd Distinctions. In *Human Resource Development Review* 8(1), 120–130. SAGE Publications Ltd. https://doi.org/10.1177/1534484309332617

Rod, B., Babaradi, A., and Gudmestad, O. T. (2016). Characteristics of arctic infrastructure resilience: Application of expert judgement. *In Twenty-Sixth (2016) International Ocean and Polar Engineering Conference,* , 26(1), 1226–1233.

Ryba, M. (2014). The Role of ICT Components in the Functioning of Critical Infrastructure. In J. Swiatkowska (Ed.), *Critical Infrastructure Security - The ICT Dimension* (1st, pp. 59–62). The Kosciuszko Institute.

Saeed, S., Altamimi, S. A., Alkyayal, N. A., Alshehri, E., Alabbad, D. A. (2023) Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors*, *23*(15), 67-79, https://doi.org/10.3390/s23156666

Sharma, M. (2017). Securing Critical Information Infrastructure Global Perspectives and Practices *(1st Ed.). Institute for Defence Studies and Analyses. ISBN: 9789382169741*

Tim, P., and Jonas, H. (2012). Measuring Resilience: Benefits and Limitations of Resilience Indices. *Journal of Risk Research* 17(3), 10-18, 10.1080/13669877.2013.808686

USA Department of Defense (DoD). (2020). Cybersecurity Maturity Model Certification (CMMC). *Chief Information Officer, U.S. Department of Defense.* https://dodcio.defense.gov/CMMC/Model/

USA Patriot Act. (2001). *USA Patriot Act Additional Reauthorizing Amendments Act of 2006 (S. 2271)*. *2005*, 1–6.

Walker, G. (2015). Come Back Sociotechnical Systems Theory, All is Forgiven. *Civil Engineering and Environmental Systems*, *32*(1–2), 170–179. https://doi.org/DOI: 10.1080/10286608.2015.1024112