World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Research Article)

Check for updates

Integrated cyber resilience strategy for safeguarding the national infrastructure of Somalia: Addressing threats

Mohamed Omar Mohamed [1, *], Osamah Mohammed Jasim [1], Ali Raad Sameer [1], Hassan Omar Ali [2] and Yahya Bare Hajon [2]

[1] *Institute of Informatics & Communication, University of Delhi South Campus, 110021 Delhi, India.*
[2] *Department of Information Technology, Delhi Technological University, 110042, Delhi, India.*

World Journal of Advanced Research and Reviews, 2023, 20(02), 1291–1299

Publication history: Received on 14 October 2023; revised on 23 November 2023; accepted on 25 November 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.20.2.2389

Abstract

In today's digital world, cyber resilience is key element for the security and steadiness of nations. It refers to the capacity to get ready for, adjust to, endure, and swiftly bounce back from cyber threats, playing a crucial role in protecting a nation's critical infrastructure. This research outlines a comprehensive cyber resilience strategy to protect Somalia's critical infrastructure from evolving cyber threats. The study analyzes the current threat landscape, identifies vulnerabilities in key sectors, and proposes a comprehensive approach. The findings of the study present a multifaceted strategy that combines inculcation, international collaboration, and recognized frameworks, forming a structured approach to identify vulnerabilities, protect critical assets, and respond effectively to cyber incidents. The proposed strategy intents to enhance Somalia's cyber resilience, offering a practical strategy for proactive defense against evolving threats and securing a digital future.

Keywords: Cyber Resılıence; Strategy; Natıonal Infrastructure; Threats; Inculcation; Somalıa

1. Introduction

In an increasingly interconnected and digitized world, the Somali government, like governments around the world, faces a growing spectrum of cyber threats that threaten the security and integrity of its critical data and digital infrastructure [1]. These threats are not limited to external actors; they extend into the insidious world of insider threats, making it even more difficult to protect sensitive government information. The need for a robust and comprehensive cyber resilience strategy is paramount.

"Cyber resilience is the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions" [2]. It is a broader concept than cybersecurity, which primarily focuses on preventing cyberattacks, and encompasses a range of practices, technologies, and strategies designed to ensure ongoing operations and recovery after an incident [3]. In the context of a secure nation, cyber resilience is directly related to the ability to defend against and recover from cyber-attacks that can have a significant impact on national security, the economy, and public safety [4]. Cyber resilience includes a comprehensive approach to protecting critical infrastructure, government systems, and sensitive information [4],[5].

Governments all around the world are realizing the value of cyber resilience in protecting national security. The United States, for example, has issued a number of executive orders and laws aimed at boosting cybersecurity and resilience in the critical infrastructure sector [6]. To increase cyber resilience, the European Union has also implemented laws such as the Network and Information Systems (NIS) Directive [7].

[*] Corresponding author: Mohamed Omar Mohamed.

As Somalia strives to modernize its public administration and provide effective digital services to citizens [8], it also faces the interconnected vulnerabilities of the digital landscape. To that end, developing a comprehensive cyber-resistance strategy that includes protection against external and internal threats is not only prudent, but also a matter of national security and public trust.

The purpose of this study is to outline the integrated strategy that make up an effective cyber-resistance tailored to the unique context and challenges of the Somali government. At a time when cyber threats are rapidly developing, the development of such strategy is essential from the point of view of information security, continuity of public service and protection of national interests.

This comprehensive strategy requires a holistic approach that takes into account technological developments, international best practices, legal frameworks and the development of human capital capable of effectively combating cyber threats. The aim of the strategy is to prevent cyber-attacks, but also to minimize their impact and facilitate a quick recovery.

The concept of "resilience" originally found its roots in the field of ecology, introduced by Canadian ecologist C.S. Holling in the 1973. He used it to describe the ability of ecosystems to absorb and recover from disturbances [9]. This concept eventually spread beyond ecology and began to be applied to various other disciplines. As information technology and cyber systems became more important in our daily lives, the concept of "resilience" began to emerge. The digital age introduced new challenges and vulnerabilities, leading to the need for resilience in the face of cyber threats. This evolution eventually gave rise to the concept of "cyber resilience" [10].

1.1. Emerging Global Cybersecurity Threats

Many national governments are dealing with serious cybersecurity issues as a result of the perceived global divide over Internet governance. They want to secure their critical infrastructure, deter criminal activity, control content, promote economic growth, and protect citizens' privacy [11]. The main source of concern is the growing number of cyberattacks. These attacks have the potential to disrupt critical infrastructure such as Industrial Control Systems, steal sensitive information, and endanger the country's security [12],[13]. Cybercriminals are also becoming more adept at attacking the supply chains that support government systems, making it difficult to keep them secure [14]. Ransomware attacks are also on the rise, in which hackers encrypt government systems and demand large sums of money to unlock them [15]. Furthermore, insider threats pose significant risks because employees, either intentionally or unintentionally, undermine security measures [16],[17],[18]. And lastly, critical infrastructure protection remains a top priority because attacks on these systems can have disastrous consequences for public safety and a country's economy. In order to preserve national security, safeguard vital infrastructure, and guarantee the continuation of vital public services in the face of evolving cyber threats, governments must be cyber resilient.

1.2. Cybersecurity Threats in Somalia

Concerns about cyber threats are growing in Somalia, as they pose serious threats to the country's stability and national security. Threats such as phishing and social engineering are becoming increasingly common in Somalia. Cybercriminals take advantage of government employees' lack of comprehensive cybersecurity training, tricking them into disclosing sensitive information or installing malware via deceptive emails and messages. This puts not only government systems at risk, but also data security, which is especially concerning given the potential impact on sensitive government data.

According to Kaspersky [19] report Somalia was listed among the top 20 countries and territories with a high risk of online infection. Malicious actors have been quick to exploit Somalia's digital vulnerabilities. The country has become an attractive target due to its limited cybersecurity infrastructure and growing reliance on digital processes and platforms.

Ransomware attacks have also emerged as a significant threat to Somalia's government. Cybercriminals target critical government entities, encrypting sensitive data and demanding ransom payments for decryption keys. Given Somalia's limited financial resources, a successful ransomware attack could be crippling, disrupting government operations and services.

“Slingshot” a sophisticated cyber-espionage threat discovered by Researchers at security firm Kaspersky, has been active in Somalia since 2012 [20]. Slingshot is infamous for its capacity to enter unnoticed and seize total control of victims' devices, it infiltrates devices via compromised routers [20].

Another major source of concern is the threat posed by extremist groups, particularly al-Shabaab, is unique. These groups restrict ICT use and prohibit Internet access in areas under their control, despite the fact that they use social media for propaganda and potential cyberattacks [1].

1.3. Somalia's current Cyber Resilience

Somalia's journey to achieve cyber resilience has been marked by both challenges and progress. Somalia faces significant cyber resilience challenges, due to the country's prolonged political instability, limited cybersecurity infrastructure, and increasingly digitalized environment. Despite these challenges, the Somali government has taken steps to improve cyber resilience. Initiatives have been launched to address the country's vulnerabilities and strengthen its digital defenses.

In May 2019, Somalia established the Somali Computer Emergency Response Team/Coordination Center (SomCERT/CC) under the National Communications Authority (NCA) [21]. SomCERT/CC is Somalia's first national/government Computer Emergency Response Team (CERT). As mentioned in [21] the primary role of SomCert/CC is to secure Somalia's cyberspace and to serve as an official point of contact for dealing with cybersecurity incidents within the Somali Internet community.

1.4. The importance of Cyber Resilience in government operations

In order to safeguard sensitive national security information, vital infrastructure, and public services from constantly evolving cyber threats, cyber resilience is of utmost importance in government operations. Ensuring the uninterrupted and secure operation of these systems is essential for maintaining public trust [22], upholding the rule of law, and protecting sensitive information.

2. Literature Review

2.1. Overview

Cyber resilience is "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources" [23]. The evolution of cyber resilience corresponds to the evolution of the internet and digital technology [24],[25],[26] . Cyber resilience has its roots in the broader field of resilience engineering, which was used to address the vulnerabilities of complex systems and the need for robust responses to unforeseen events [27]. As highlighted by [28] the understanding of cyber resilience has evolved to include not only technical aspects but also organizational, human and strategic dimensions of cybersecurity. In an increasingly digital world, a comprehensive cyber resilience framework is critical for ensuring a nation's security and stability [29]. A framework of this type includes a variety of strategies, practices, and policies that all contribute to a secure nation.

2.2. Existing Cyber Resilience frameworks

2.2.1. NIST Framework

NIST's *v1.1* [30] is framework that offers voluntary guidance, including standards, guidelines, and practices, aimed at managing and enhancing cybersecurity for critical infrastructure. The framework, was released in response to growing cyber threats, provides a comprehensive, risk-based approach to managing cybersecurity risks. It is organized around three main components: The Framework Core, which outlines key cybersecurity activities and outcomes; the Framework Implementation Tiers, which guide organizations in managing and adapting their cybersecurity practices; and the Framework Profiles, which allow organizations to tailor their approach based on specific risk considerations and needs. By promoting a flexible, risk-informed strategy, the framework enables organizations to improve their cybersecurity posture, fostering resilience and adaptability in the face of an ever-changing threat landscape. NIST is currently in the process of developing the highly awaited version 2.0 of the Cybersecurity Framework. This initiative stems from a clear recognition of the necessity to adjust to new challenges and technological progress [31].

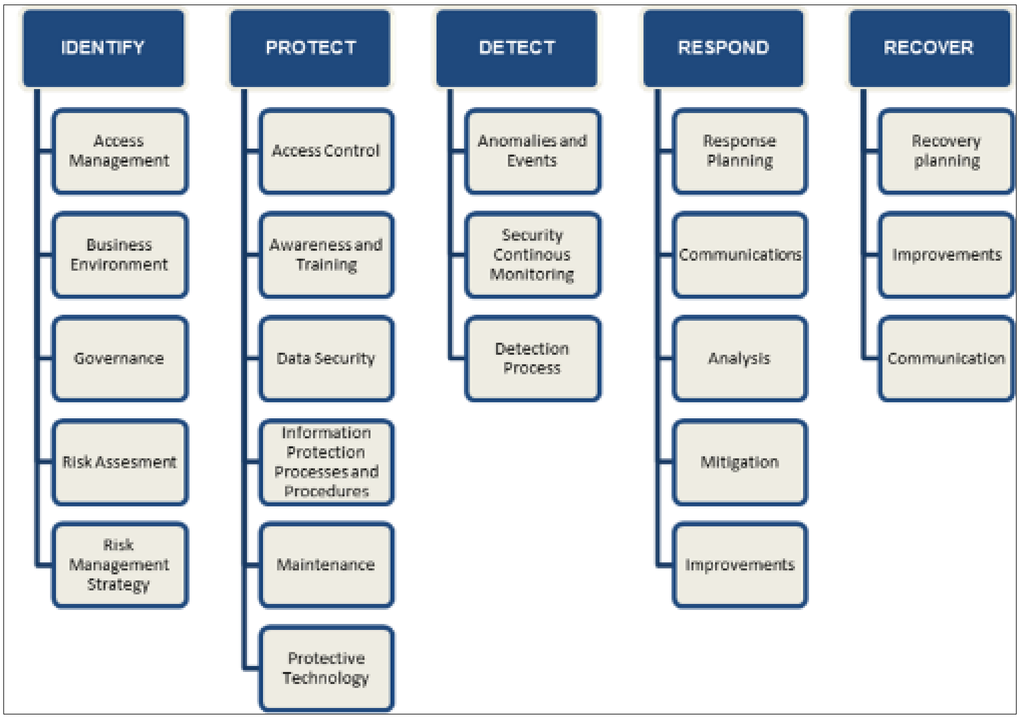

Figure 1 NIST Framework

2.3. MITRE Cyber Resilience Engineering Framework

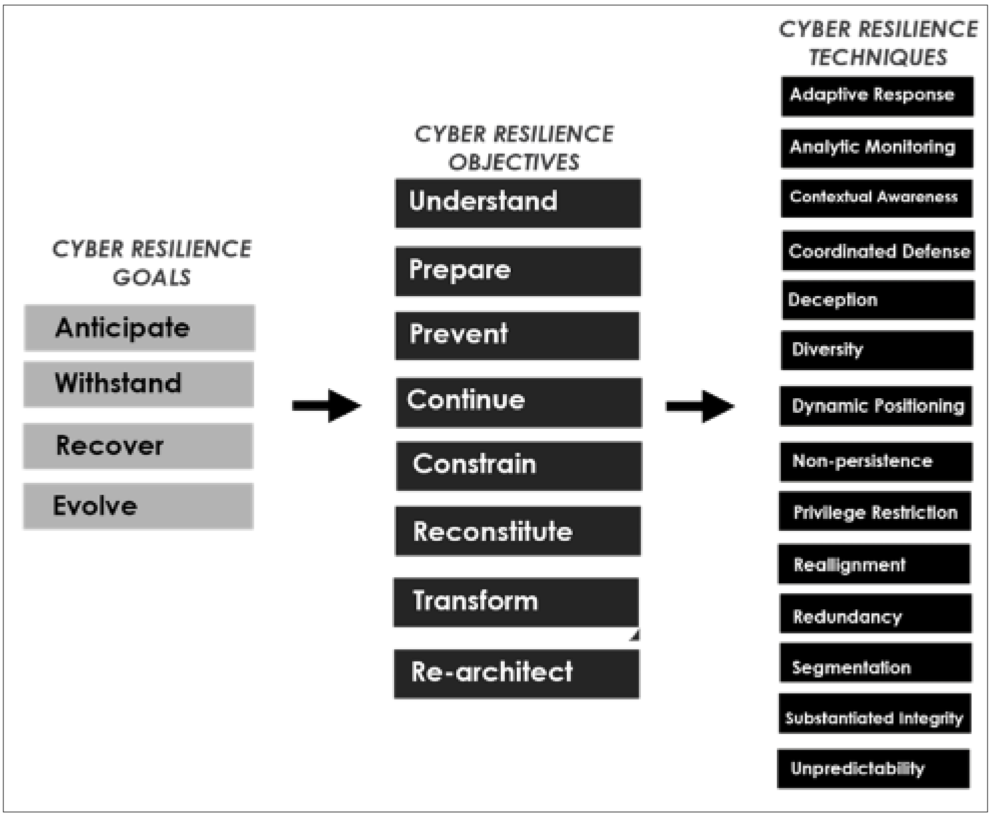

Figure 2 Cyber Resiliency Engineering Framework

MITRE's Cyber Resiliency Engineering Framework (CREF) [32], developed around 2011, serves as a strategic tool for effectively managing cyber threats. As illustrated in **Figure 2,** this framework is based on four primary goals: anticipating potential threats, withstanding attacks, recovering business functions after an attack, and adapting functions to minimize impact. CREF provides a comprehensive set of resilience-focused objectives, practices, costs, and metrics, leveraging concepts from resilience engineering, mission assurance engineering, and cybersecurity.

2.4. Cyber Resilience Goals to Objectives

Table 1 Mapping Cyber Resilience Goals to Objectives [32]

	Understand	Prepare	Prevent	Continue	Constrain	Reconstitute	Transform	Re-architect
Anticipate	√	√	√					
Withstand	√			√	√	√		
Recover	√			√				
Evolve	√						√	√

As demonstrated in **Table 1**, "Anticipate" involves understanding, preparing and preventing which simply means gaining insights, getting ready, and taking preventative measures against cyberattacks. "Withstand" seeks to understand the challenges posed by cyber threats while also ensuring the continuity of critical operations. Within "Recover" goal, the associated objectives encompass Understanding, continuity, Constrain and reconstitute. This includes not only determining the scope of the damage and disruptions caused by a cyberattack, but also ensuring the uninterrupted continuation of critical operations. Furthermore, it entails limiting the negative effects and then reconstituting affected systems and functions, ultimately working towards a comprehensive recovery strategy. The objectives of the "Evolve" goal include understanding, transforming, and reconfiguring. This comprises learning about the changing landscape, adapting to changes, and making architectural improvements.

Taken together, these goals and objectives form a comprehensive framework that helps to strengthen national cybersecurity. This framework is intended to ensure the uninterrupted functioning of critical operations and the rapid recovery from cyber threats on a national scale. The goals and objectives work in tandem to improve the nation's overall cyber resilience.

2.5. Cyber Resilience Techniques to Objectives

Table 2 Mapping Cyber Resilience Techniques to Objectives

	Understand	Prepare	Prevent	Continue	Constrain	Reconstitute	Transform	Re-architect
Adaptive Response				√	√	√		
Analytic Monitoring	√	√			√	√		
Contextual Awareness								
Coordinated Protection		√	√	√	√			
Deception	√		√		√			
Diversity			√	√				√
Dynamic Positioning	√		√	√				√
Non-persistence			√	√	√			√
Privilege Restriction			√		√			
Realignment					√		√	

Redundancy				√		√		
Segmentation			√		√			
Substantiated Integrity	√			√	√	√		
Unpredictability	√		√	√				

Table 2 outlines the alignment between cyber resiliency objectives and the specific techniques employed. It serves as a valuable reference, illustrating how distinct techniques correspond to the achievement of the objectives in strengthening resilience against cyber threats and disruptions.

3. The Research Strategy

To strengthen Somalia's cyber resilience, this study proposes a strategy that combines the introduction of an innovative concept of inculcation, international collaboration, and the implementation of existing frameworks such as NIST's [30] and the MITRE's [32].

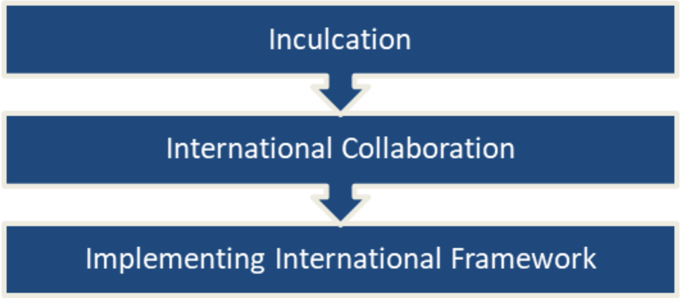
Inculcation
International Collaboration
Implementing International Framework

Figure 3 Key factors

3.1. Inculcation

Introducing the idea of "Inculcation" as a strategy for boosting Somalia's cybersecurity resilience. Inculcation in this context means actively promoting a culture where everyone is aware and careful about cybersecurity. This involves ongoing education, awareness campaigns, and making cybersecurity part of daily routines, aiming to create a proactive and watchful mindset among individuals and organizations.

The key strength of Inculcation lies in its potential to bring about several positive changes in Somalia's cybersecurity approach. Firstly, it aims to significantly lower the risk of cyber threats. By educating the workforce on identifying and handling potential risks, it helps strengthen overall cybersecurity. Secondly, by making cybersecurity practices a regular part of daily operations, Inculcation not only helps in preventing cyber threats but also sets up a resilient environment that can recover quickly after an incident. This proactive approach aligns with the idea that achieving cyber resilience requires a cultural shift where everyone shares the responsibility for cybersecurity.

The benefits of Inculcation go beyond just dealing with immediate cyber threats. It nurtures a group of cybersecurity advocates within Somalia's workforce. These advocates, armed with knowledge from Inculcation, become crucial assets in the ongoing battle against evolving cyber threats. The synergy between increased individual awareness and making cybersecurity a routine part of operations puts Somalia on a path not only to achieve cyber resilience but also to create a lasting and adaptable cybersecurity approach. Inculcation, as a new and innovative idea, becomes a key player in shaping a secure digital future for Somalia.

3.2. International Collaboration

International collaboration is fundamental for Somalia's cyber resilience strategy, recognizing the interconnected nature of global cybersecurity challenges. Creating partnerships with international organizations, neighboring countries, and cybersecurity alliances is paramount. Actively engaging with entities such as the United Nations, the African Union, and regional cybersecurity forums facilitates the sharing of critical threat intelligence, best practices, and collaborative response mechanisms. This global collaboration establishes a collective defense front, ensuring that

Somalia remains informed about emerging cyber threats and can contribute to the collective efforts in tackling transnational cybercrime. Somalia's cyber resilience strategy should involve active participation in international cybersecurity initiatives and conventions. Additionally, engaging in joint cybersecurity exercises, capacity-building programs, and collaborative research projects with international partners further enhances Somalia's cybersecurity capabilities. By being an active contributor to the global cybersecurity community, Somalia positions itself to benefit from shared expertise, technological advancements, and collective efforts to mitigate the impact of cyber threats on a global scale.

3.3. Implementing Existing International Framework

Implementing existing cybersecurity frameworks in Somalia, despite facing challenges, is crucial for enhancing the nation's digital resilience. The adoption of established frameworks like the NIST Cybersecurity Framework and the MITRE Cyber Resiliency Engineering Framework provides a structured and recognized approach to tackling cyber threats. These frameworks offer guidelines for identifying vulnerabilities, protecting critical assets, and responding effectively to incidents. Moreover, incorporating these frameworks into Somalia's cybersecurity policies and practices requires a concerted effort to build awareness and capacity. Conducting training programs and awareness campaigns can ensure that individuals at all levels understand the importance of cybersecurity and are equipped to implement the frameworks effectively. Collaborative efforts between the government, private sector, and educational institutions can play a vital role in overcoming implementation challenges, creating a more cyber-resilient environment for Somalia.

3.4. Implementation Challenges and Recommendations

Challenges such as limited resources, technical expertise, and awareness may hinder the implementation process. To overcome these obstacles, Somali government can prioritize phased implementation, focusing on the most critical aspects first and gradually expanding as resources permit. Additionally, fostering partnerships with international organizations and seeking external assistance can provide valuable support in navigating these challenges. In moving forward, it is essential for stakeholders, including government bodies, private enterprises, and educational institutions, to collaborate closely in implementing and sustaining these initiatives.

4. Conclusion

The research highlights the significance of utilizing a diverse strategy to enhance Somalia's cyber resilience. By introducing the concept of inculcation, our aim is to create a culture where cybersecurity is ingrained in everyday practices, developing a proactive stance against evolving cyber threats. Simultaneously, fostering international collaboration and implementing established frameworks like NIST and the MITRE's Cyber Resiliency Engineering Framework form a solid foundation for a resilient cybersecurity strategy. These measures, when combined, provide a comprehensive and practical strategy to navigate the complex and dynamic landscape of cyber threats, positioning Somalia for a more secure and digitally resilient future.

Continuous awareness, international cooperation, and the adoption of proven frameworks will be essential in creating a cyber-resilient Somalia. By embracing these strategies, the nation can strengthen its defenses, adapt to emerging cyber challenges, and cultivate a secure digital environment for its citizens and organizations.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] I. Gagliardone and N. Sambuli, "Cyber Security and Cyber Resilience in East Africa," *Cent. Int. Gov. Innov. Chatham House*, no. 15, pp. 1–16, 2015.

[2] NIST SP800-53, "Security and Privacy Controls for Information Systems and Organizations," *NIST Spec. Publ.*, p. 465, 2020, [Online]. Available: https://doi.org/10.6028/NIST.SP.800-53r5

[3] "Cyber Resilience | PNNL." Accessed: Oct. 16, 2023. [Online]. Available: https://www.pnnl.gov/explainer-articles/cyber-resilience

[4] H. Tiirmaa-Klaar, “Building national cyber resilience and protecting critical information infrastructure,” *J. Cyber Policy*, vol. 1, no. 1, pp. 94–106, Jan. 2016, doi: 10.1080/23738871.2016.1165716.

[5] D. J. C. and W. W. J. W. and J. van Vuuren, *Building Cyber Reslience in Africa*. 2017.

[6] “National Infrastructure Protection Plan and Resources | CISA.” Accessed: Oct. 16, 2023. [Online]. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/national-infrastructure-protection-plan-and-resources

[7] D. Markopoulou, V. P.-... L. & S. Review, and undefined 2019, “The new EU cybersecurity framework: The NIS Directive, ENISA’s role and the General Data Protection Regulation,” *Elsevier*, Accessed: Oct. 16, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0267364919300512

[8] A. Sagar, “DIGITAL ID : Prospects And Challenges For Somalia - Heritage Institute,” Heritage Institute. Accessed: Oct. 16, 2023. [Online]. Available: https://heritageinstitute.org/digital-id-prospects-and-challenges-for-somalia/publications/

[9] A. Mcaslan, “THE CONCEPT OF RESILIENCE Understanding its Origins, Meaning and Utility A strawman paper,” 2010, Accessed: Nov. 07, 2023. [Online]. Available: www.resalliance.org

[10] R. B. Stafford and C. L. Bouwens, “DESIGNING SYSTEMS FOR CYBER RESILIENCE,” 2018.

[11] S. J. Shackelford and A. N. Craig, “Beyond the new ‘digital divide’: Analyzing the evolving role of national governments in Internet governance and enhancing cybersecurity,” *Stanford J. Int. Law*, vol. 50, no. 1, pp. 119–184, 2014.

[12] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, “A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services,” *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018, doi: 10.1109/COMST.2018.2855563.

[13] M. Abomhara and G. M. Køien, “Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks,” *J. Cyber Secur. Mobil.*, vol. 4, no. 1, pp. 65–88, 2015, doi: 10.13052/jcsm2245-1439.414.

[14] J. Aberman, “Emerging paradigms of cybercrimes, supply chain attacks, and national security ramifications.,” no. December, 2022.

[15] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, “Ransomware: Recent advances, analysis, challenges and future research directions,” *Comput. Secur.*, vol. 111, p. 102490, Dec. 2021, doi: 10.1016/J.COSE.2021.102490.

[16] G. Mazzarolo and A. D. Jurcut, “Insider threats in Cyber Security: The enemy within the gates,” Nov. 2019, Accessed: Oct. 23, 2023. [Online]. Available: https://arxiv.org/abs/1911.09575v1

[17] P. Legg *et al.*, “Towards a conceptual model and reasoning structure for insider threat detection,” *J. Wirel. Mob. Networks, Ubiquitous Comput. Dependable Appl.*, vol. 4, no. 4, pp. 20–37, 2013.

[18] C. L. Hartline, “EXAMINATION OF INSIDER THREATS: A GROWING CONCERN,” 2017.

[19] Expert Kaspersky, “Kaspersky Security Bulletin 2020-2021. EU statistics,” *Secur. by Kaspersky*, 2021, [Online]. Available: https://securelist.com/kaspersky-security-bulletin-2020-2021-eu-statistics/102335/

[20] “Kaspersky / Press release | Africa & Middle East: Slingshot, the spy that came in from the router.” Accessed: Nov. 02, 2023. [Online]. Available: https://kaspersky.africa-newsroom.com/press/slingshot-the-spy-that-came-in-from-the-router?lang=en

[21] “Introduction | SOMCERT.” Accessed: Nov. 20, 2023. [Online]. Available: https://somcert.gov.so/introduction/

[22] A. M. Ronchi, “Cyber Resilience, its Relevance, and Cyber Capacity Building,” pp. 1–6, 2023, Accessed: Nov. 21, 2023. [Online]. Available: https://re.public.polimi.it/handle/11311/1234903

[23] S. PETRENKO, *CYBER RESILIENCE*. RIVER PUBLISHERS, 2023. Accessed: Oct. 19, 2023. [Online]. Available: https://www.routledge.com/Cyber-Resilience/Petrenko/p/book/9788770229715

[24] H. Boyes, “Cybersecurity and Cyber-Resilient Supply Chains,” *Technol. Innov. Manag. Rev.*, vol. 5, no. 4, pp. 28–34, 2015, doi: 10.22215/timreview888.

[25] I. Linkov and A. Kott, “Fundamental Concepts of Cyber Resilience: Introduction and Overview,” *Cyber Resil. Syst. Networks*, pp. 1–25, 2019, doi: 10.1007/978-3-319-77492-3_1/COVER.

[26] D. Galinec and W. Steingartner, “Combining cybersecurity and cyber defense to achieve cyber resilience,” *2017 IEEE 14th Int. Sci. Conf. Informatics, INFORMATICS 2017 - Proc.*, vol. 2018-Janua, pp. 87–93, Jul. 2018, doi: 10.1109/INFORMATICS.2017.8327227.

[27] I. Linkov and Alexander Kott, “Fundamental Concepts of Cyber Resilience: Introduction and Overview,” *Cyber Resil. Syst. Networks*, 2018.

[28] C. Ciuchi, “Developing a Comprehensive Model for Digital Lifelong Learning Using Cyber Resilience Framework,” vol. IX, pp. 105–112, 2022, doi: 10.19107/cybercon.2022.14.

[29] O. Kayode-ajala, “Establishing Cyber Resilience in Developing Countries : An Exploratory Investigation into Institutional , Legal , Financial , and Social Challenges,” pp. 1–10.

[30] National Institute of Standards And Technology, “Framework for Improving Critical Infrastructure Cybersecurity 重要インフラのサイバーセキュリティを 改善するためのフレームワーク,” 2018, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf%0Ahttps://doi.org/10.6028/NIST.CSWP.04162018

[31] N. I. of S. and Technology, “The NIST Cybersecurity Framework 2.0 (Draft),” Aug. 2023, doi: 10.6028/NIST.CSWP.29.IPD.

[32] D. Bodeau, R. Graubart, J. Picciotto, and R. McQuaid, *Cyber Resiliency Engineering Framework*, no. September. 2012. [Online]. Available: http://www.mitre.org/work/tech_papers/2012/11_4436/%5Cnpapers2://publication/uuid/F03D9287-780F-4B61-AC47-E77BEDC3F939