Scientific and Practical Cyber Security Journal (SPCSJ) 8(1): 69 – 75 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

A MULTI-PRONGED FRAMEWORK FOR A CYBER-SECURE NIGERIA

Ahmed Abubakar Aliyu[1,2]
[1] School of Cyber Science and Engineering, Wuhan University, Wuhan, China, 430072
[2] Faculty of Computing, School of Science, Computing and Engineering, Kaduna State University, Kaduna 800283, Nigeria

ABSTRACT. The digital revolution has presented significant opportunities, but it has also introduced new threats, such as cybercrime. Nigeria is facing substantial cyber threats, which cost billions of Naira and impact individuals and businesses. The challenges include inadequate awareness, weak legal frameworks, limited digital literacy, and poor cyber hygiene. To enhance cybersecurity in Nigeria, a multi-pronged approach is necessary. This includes advanced cybersecurity tools, robust legal frameworks, education campaigns, capacity building, and public-private partnerships. Success stories from other countries, such as Singapore and Kenya, offer valuable lessons for Nigeria. Therefore, this paper proposes a multi-pronged framework to improve cybersecurity in Nigeria. By adopting these frameworks and best practices as well as working together, Nigeria can create a secure and prosperous digital future.

KEYWORDS: Cybersecurity, Digital literacy, National Security, Cyber Crime, Cyber hygiene

1. INTRODUCTION

The digital revolution has profoundly changed our lives, affecting the way we connect and do business, changing the way we live, the way we connect, and the way we do business as technology has become an integral part of our existence. In Nigeria, the digital sphere offers tremendous opportunities for economic growth, social development, and individual empowerment [1]. However, this connectivity also exposes us to new threats, such as the ever-evolving realm of cybercrime. As new technologies emerge, cybercriminals are constantly adapting and innovating, developing sophisticated methods to exploit vulnerabilities and cause devastating damage [2]. Cybercrime covers a wide range of activities, from online fraud and data breaches to malware attacks and cyber espionage, and its impact is far-reaching and diverse. Businesses suffer significant financial and reputational losses, individuals lose their hard-earned savings and sensitive information, and critical infrastructure is compromised, posing a threat to public safety and national security. In the face of escalating threats, a robust and proactive cybersecurity posture in Nigeria is more important than ever [3]. This is not only a technical challenge, but also a societal imperative. Achieving a cyber-secure Nigeria requires a holistic approach that goes beyond technological solutions. It requires collaboration, awareness, and a commitment to fostering a culture of cybersecurity at all levels of society.

The Cyber Security Experts Association of Nigeria (CSEAN) National Cyber Threat Forecast 2023 paints a concerning picture for Nigeria's cybersecurity landscape [4]. The report anticipates a rise in ransomware attacks targeting both public and private entities, alongside growing concerns about misinformation campaigns and attacks on vulnerable government assets. Furthermore, the potential

for insider threats, potentially involving malicious use of Artificial Intelligence, raises additional concerns. The report emphasizes the need for collaboration between individuals, organizations, and law enforcement to combat these evolving threats and build a safer digital environment. This necessitates proactive security measures and continuous vigilance from all stakeholders in Nigeria. Table 1 compares some top cybercrime around the world based on the MSSPAleart cybersecurity list and annual research.

Tab. 1. Comparative overview of some cybercrime concerns

Country	Ranking	Key Concerns	Notes
China	1	High number of cyberattacks, often targeting critical infrastructure	Data breaches, espionage, intellectual property theft
Brazil	5	High volume of cybercrime targeting the financial sector	Banking fraud, credit card scams, data breaches
United States	10	High volume of cybercrime incidents due to extensive digital infrastructure	Phishing attacks, malware infections, identity theft
Russia	N/A	High prevalence of cybercrime actors and activity	Ransomware attacks, disinformation campaigns, online fraud
Nigeria	16	High volume of cybercrime targeting individuals and businesses	Online scams (e.g., romance scams), phishing attacks, malware infections

This study examines the complex landscape of cybercrime in Nigeria. It analyses the evolving threats, assesses the current state of cybersecurity, and identifies the vulnerabilities that require immediate attention. It also explores potential solutions and strategies to build a cyber-secure nation and ensure a prosperous digital future for the next generation. The study aims to encourage stakeholders in government, the private sector, civil society, and academia to recognize the urgency of addressing cyber threats. It advocates a multi-pronged approach that includes proactive defense mechanisms, robust regulatory frameworks, comprehensive awareness campaigns, and investment in critical cybersecurity infrastructure.

2. PREVALENCE AND IMPACT OF CYBERCRIME IN NIGERIA

Cybercrime is a significant and growing threat in Nigeria, affecting individuals, businesses, and the nation as a whole [5]. Understanding its prevalence and impact is critical to developing effective strategies to combat this evolving threat. This paper provides a statistical snapshot: As cybercrime is estimated to cost the world about $7 billion, it costs Nigeria over $500 million annually, representing a significant drain on the country's economy[6]. In 2021 alone, Nigeria experiences 14.7 million cyber-attacks, the highest in Africa and the seventh highest in the world. Individuals aged 18-34 are particularly vulnerable, accounting for 60% of cybercrime victims. Online scams such as 'Yahoo Yahoo' scams, romance scams, and phishing attacks targeting bank accounts and sensitive information are widespread. Data breaches are also an issue. The National Identity Management Commission (NIMC) database breach in 2019 exposed the personal information of over 50 million Nigerians. Ransomware attacks, which target businesses and critical infrastructure, are increasingly common. Online platforms are often used for cyberbullying and harassment of individuals, especially women and children [7]. These are just a few examples of the diverse and pervasive nature of cybercrime in Nigeria. The CSEAN predicts that there will be an increase in insider threats in Nigeria in 2024 due to the malevolent use of artificial intelligence [8]. The consequences can be devastating, ranging from financial loss and identity theft to emotional distress

and reputational damage. Several factors contribute to the prevalence and impact of cybercrime in Nigeria, including a lack of cybersecurity awareness. Many Nigerians lack basic knowledge about cyber threats and how to protect themselves online.

Nigeria faces a significant challenge with inadequate cybersecurity awareness among its citizens, who often lack basic knowledge about cyber threats and how to protect themselves online. Furthermore, the country's cybercrime laws are still evolving, resulting in gaps and challenges in enforcement [9]. Limited access to technology and a lack of digital literacy skills can impede individuals' ability to protect themselves online. Poor cyber hygiene practices, such as weak passwords, insecure Wi-Fi networks, and the use of pirated software, can increase vulnerability to cyber-attacks. To address these vulnerabilities, a multi-pronged approach is necessary. This includes raising cybersecurity awareness through public education campaigns, community outreach programs, and school curricula. Equipping Nigerians with the knowledge and skills to stay safe online is crucial. Additionally, it is important to strengthen the legal framework by implementing robust cybercrime laws with clear definitions, effective enforcement mechanisms, and proportionate penalties to deter cybercriminals. Promoting digital inclusion is crucial. Nigerians can be empowered to participate in the digital world safely and securely through affordable internet access, technology training programs, and digital literacy initiatives. To reduce the risk of cyber-attacks, it is important to promote strong passwords, secure Wi-Fi networks, and responsible online behavior.

Moreover, a report by leading cybersecurity professionals has anticipates a significant rise in cyber threats throughout 2024. The report urges individuals, organizations, and governmental bodies to adopt a proactive and vigilant approach to safeguarding cyberspace. One of the most concerning trends highlighted in the report is the anticipated surge in ransomware attacks. Malicious software programs, designed to lock or encrypt critical data and demand ransom payments for its recovery, are expected to continue targeting both public and private entities across diverse sectors. This poses a significant threat to national security, economic stability, and individual privacy, as successful attacks can disrupt critical operations, lead to financial losses, and expose sensitive information. Moreover, the report highlights the increasing danger of misinformation and disinformation campaigns. Malicious actors are using digital platforms more and more to spread false or misleading information, with the aim of manipulating public opinion, causing division, and eroding trust in institutions. This can have serious consequences, hindering informed decision-making, exacerbating social divisions, and potentially threatening national security. There are concerns regarding the vulnerability of government online assets. As the public sector increasingly relies on digital infrastructure, government websites and databases become more attractive targets for cybercriminals. These attacks can aim to disrupt critical services, steal sensitive data, or manipulate information for malicious purposes. This underscores the need for strong cybersecurity measures in government agencies to safeguard the security and integrity of critical infrastructure. Furthermore, the growing concern of insider threats, particularly with the potential integration of Artificial Intelligence (AI) in cyberattacks, disgruntled employees or individuals with authorized access to sensitive information pose a significant risk as well as malicious actors may exploit insider access to orchestrate sophisticated attacks. Therefore, robust access control mechanisms, employee education, and continuous monitoring within organizations are necessary.

3. MULTI-PRONGED FRAMEWORK PROPOSAL

Cybersecurity has become a critical national imperative for Nigeria due to the country's increasing reliance on digital infrastructure. A multi-pronged framework approach is required to combat the evolving threat landscape, which requires a mix of technological advancements, robust regulatory

frameworks, proactive education, and collaborative efforts among various stakeholders. Investing in advanced cybersecurity tools and building a robust cybersecurity workforce is both fundamental to ensuring effective cybersecurity. Capacity building in this area is essential. This includes the deployment of intrusion detection and prevention systems (IDS/IPS), security information and event management (SIEM) tools, and threat intelligence platforms [10]. It is also essential to strengthen critical infrastructure with secure hardware, software, and network architecture. Improve incident response capabilities, including rapid threat identification. Strong legal frameworks serve as a deterrent and ensure accountability. Nigeria should regularly review and update its cybercrime laws to keep pace with evolving threats and modus operandi. It is essential to have clear definitions of cybercrimes, proportionate penalties, and effective enforcement mechanisms. Working with international partners to develop harmonized cybercrime legislation will enhance global security and facilitate cross-border investigations.

Implementing national awareness campaigns through a variety of channels, from traditional media to targeted online platforms, is critical. These campaigns should educate individuals and businesses about common cyber threats, phishing tactics, password hygiene, and safe online practices. Integrating cybersecurity education into school curricula will equip future generations with the knowledge and skills necessary to navigate the digital world safely. Building a robust cybersecurity workforce which requires investment in training and development programs to create a skilled pool of cybersecurity professionals is essential. Specialized training in areas such as digital forensics, incident response, threat analysis, and vulnerability assessment is essential. Establishing centers of excellence for cybersecurity research and innovation can further propel Nigeria to become a regional leader in the field.

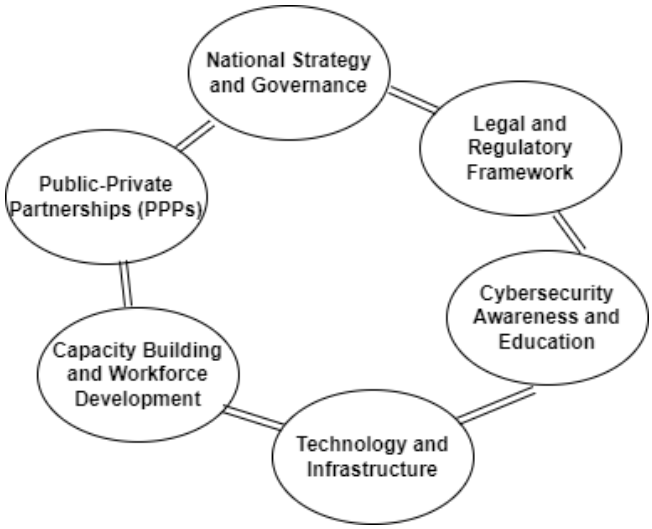

Fig. 1. Multi-Pronged Framework Proposal

As depicted in Figure 1, Public-private partnerships (PPPs) are powerful drivers of cyber resilience. Establishing formal platforms for collaboration between government agencies, private sector entities, and civil society organizations promotes knowledge sharing, resource pooling, and coordinated responses to cyber threats. Leveraging the expertise and resources of the private sector enhances technological capabilities and incident response agility. Civil society organizations play a critical role in raising awareness, advocating for stronger regulatory frameworks, and empowering vulnerable communities. Through this multi-pronged approach, Nigeria can chart a path to cyber resilience. Through technological fortification, robust legal frameworks, proactive education, capacity building, and collaborative synergies, the country can protect its digital assets,

foster trust in its digital economy, and empower its citizens to navigate the digital world with confidence. Table 2 explains the Multi-Pronged Framework proposal description.

Tab. 2. Multi-Pronged Framework description

Framework Component	Description	Example Initiatives
National Strategy and Governance	Develop a comprehensive national cybersecurity strategy with clear goals, priorities, and action plans. Establish a dedicated cybersecurity agency or department to oversee implementation.	Develop a national cybersecurity strategy in line with Singapore's model. - Establish a National Cybersecurity Center to coordinate efforts across government agencies.
Legal and Regulatory Framework	Enact robust cybercrime laws with clear definitions of offenses, proportionate penalties, and effective enforcement mechanisms. Strengthen data protection regulations and promote international cooperation on cybercrime.	Implement mandatory data breach notification laws similar to the EU's GDPR. - Collaborate with Interpol and ITU on cyber threat intelligence sharing and capacity building.
Cybersecurity Awareness and Education	Implement nationwide awareness campaigns to educate individuals and businesses about cyber threats, best practices, and personal responsibility. Integrate cybersecurity education into school curriculums.	Launch public awareness campaigns through diverse channels like TV, radio, and social media. - Develop age-appropriate cybersecurity curricula for schools.
Technology and Infrastructure	Invest in advanced cybersecurity tools and technologies, including intrusion detection and prevention systems (IDS/IPS), security information and event management (SIEM) tools, and threat intelligence platforms. Secure critical infrastructure and government systems.	Modernize government IT infrastructure with secure hardware, software, and network architecture. - Establish a national cyber incident response center.
Capacity Building and Workforce Development	Train and develop a skilled workforce of cybersecurity professionals through specialized training programs in areas like digital forensics, incident response, threat analysis, and vulnerability assessment.	Establish centers of excellence for cybersecurity research and innovation. - Partner with universities and private sector companies to offer cybersecurity training programs.
Public-Private Partnerships (PPPs)	Foster collaboration between government agencies, private sector entities, and civil society organizations to share resources, expertise, and best practices. Encourage joint initiatives to address cyber threats and build cyber resilience.	Establish platforms for dialogue and information sharing between stakeholders. - Partner with private companies to develop and deploy innovative cybersecurity solutions.

4. ADAPTING BEST PRACTICES

Singapore's Cyber Security Agency (CSA) is a model of effective public-private partnership (PPP) in cyber security. The CSA actively works with private companies and civil society organizations on initiatives such as awareness campaigns, threat intelligence sharing, and talent development. This collaborative approach has significantly improved Singapore's cyber resilience. Estonia's X-Road data exchange platform is another secure data exchange platform that enables seamless and secure information sharing between government agencies, businesses, and citizens. Its

decentralized architecture and strong encryption protocols offer valuable lessons for Nigeria in building a secure government information infrastructure. In Africa, Kenya's Cybercrime Unit is a specialized unit within the Directorate of Criminal Investigations that focuses on investigating and prosecuting cybercrime [11]. Its success in securing convictions and raising awareness has deterred cybercriminals and fostered a culture of cybersecurity in Kenya.

Develop a national cybersecurity strategy: Inspired by Singapore's comprehensive national cybersecurity strategy, Nigeria can articulate a clear vision, strategic priorities, and concrete action plans for building cyber resilience.

Establish a cybercrime task force: Similar to Kenya's dedicated cybercrime unit, Nigeria can create a specialized task force with law enforcement, technical experts, and legal professionals to effectively investigate and prosecute cybercrimes in addition to The Nigerian Computer Emergency Response Team which was established in the Office of the National Security Adviser.

Implement mandatory data breach notification laws: Following the European Union's General Data Protection Regulation (GDPR), Nigeria can implement mandatory data breach notification laws to hold organizations accountable for protecting personal data and informing individuals of security breaches.

Promoting digital literacy through public-private partnerships: Collaborations between government agencies, NGOs, and telecommunications companies can implement targeted digital literacy initiatives through mobile phone subscriptions, community centers, and school curricula.

Facilitating regional and international collaboration: Engaging in knowledge sharing and joint initiatives with other African nations and international organizations such as Interpol and ITU can enhance cyber threat intelligence sharing, capacity building, and coordinated responses to cross-border cybercrime.

5. CONCLUSION

The specter of cyber threats casts a long shadow over our increasingly interconnected world, and Nigeria stands at a critical juncture. The nation faces a stark choice: succumb to the vulnerabilities of cyberspace or forge a path towards a secure and prosperous digital future which is a call to action that cannot be ignored. Cybercrime flourishes in the digital shadows, inflicting significant economic losses, jeopardizing national security, and eroding trust in the online ecosystem. Data breaches expose the sensitive information that forms the bedrock of our digital identities, while malware infections cripple essential infrastructure and disrupt vital services. These are not distant threats; they are the harsh realities confronting the global community, and Nigeria is not immune. Yet, amidst these challenges, a glimmer of hope remains. Nigeria boasts a vibrant and resilient population, a burgeoning technology sector brimming with innovation, and a growing understanding of the critical need for cybersecurity [12]. These factors provide the foundation upon which the nation can not only overcome cyber threats but thrive in the digital age. Imagine a Nigeria where businesses operate with unwavering confidence, secure in the knowledge that their data and transactions are protected. Imagine citizens navigating the digital realm with unbridled curiosity, empowered by knowledge and shielded by a robust legal framework. Imagine a future where young minds, unfettered by the fear of cyber-attack, harness the power of technology to solve the pressing societal challenges that confront the nation. This is the vision for Nigeria's digital future, a future that must be collectively built. But this vision cannot be realized through individual efforts alone. It necessitates a collective endeavor, a unified voice rising against the shadows of cyber threats. This necessitates unwavering commitment from governments to enact robust cybercrime

legislation, invest in vital infrastructure, and foster a culture of cyber awareness. It requires the ingenuity of the private sector to develop cutting-edge security solutions and foster a thriving cybersecurity ecosystem. It necessitates the dedication of educators to equip future generations with the skills and knowledge to navigate the digital landscape with confidence. Finally, and most importantly, it demands the active participation of every citizen, young and old, to adopt safe online practices and champion the cause of cyber resilience. This is not just a fight against a faceless enemy; it is a fight for the very foundation of Nigeria's digital future. To secure this future, the nation must move forward with unity and purpose, embracing the collective responsibility of building a cyber-secure Nigeria. Let the world witness not the echoes of vulnerability, but the resounding anthem of a nation that refuses to be defined by cyber threats, but rather empowered by the boundless possibilities of the digital age. Together, this vision of a safer, more secure, and prosperous Nigeria can be achieved, where technology becomes a force for good, not a weapon of darkness. Let this be the digital legacy of this generation, a testament to the enduring spirit of resilience that defines the nation.

REFERENCES:

[1] K. Njenga, *Information Systems Security in Small and Medium-Sized Enterprises: Emerging Cybersecurity Threats in Turbulent Times*. 2022. doi: 10.52305/KSVB7323.

[2] A. A. Aliyu, "Improving Cloud Data Security by hybridization of Zero-Knowledge Proof and Time-Based One-Time Password," *KASU J. Math. Sci. KJMS*, vol. 1, no. 2, pp. 116–126, Dec. 2020.

[3] T. Akinyetun, "Poverty, Cybercrime and National Security in Nigeria," *J. Contemp. Sociol. Issues*, vol. 1, pp. 1–23, Aug. 2021, doi: 10.19184/csi.v1i2.24188.

[4] C. Kanu *et al.*, "Frauds and forgeries in banking industry in Africa: a content analyses of Nigeria Deposit Insurance Corporation annual crime report," *Secur. J.*, vol. 36, no. 4, pp. 671–692, Dec. 2023, doi: 10.1057/s41284-022-00358-x.

[5] J. Garba, J. Kaur, and E. N. M. Ibrahim, "Awareness of cybercrime among online banking users in Nigeria," *Niger. J. Technol.*, vol. 42, no. 3, pp. 406–413, Nov. 2023, doi: 10.4314/njt.v42i3.14.

[6] S. Olomu, "Nigeria tightens laws to tackle yearly cyber-crime losses of $500m," ITWeb Africa. Accessed: Mar. 04, 2024. [Online]. Available: https://itweb.africa/content/mYZRXM9gxVNvOgA8

[7] B. Sule, M. Yahaya, U. Sambo, and B. Mat, "Cybersecurity and Cybercrime in Nigeria: The Implications on National Security and Digital Economy," vol. 4, pp. 27–61, Oct. 2021.

[8] S. Odeniyi, "Nigeria to witness high cyber threats in 2024 – Report," Punch Newspapers. Accessed: Mar. 02, 2024. [Online]. Available: https://punchng.com/nigeria-to-witness-high-cyber-threats-in-2024-report/

[9] A. A. Abubakar and A. U. Shamsuddeen, "Information Security: An Effective Tool For Sustainable Nigerian National Security And Development," *Sci. Pract. Cyber Secur. J.*, 2023, Accessed: Apr. 18, 2023. [Online]. Available: https://journal.scsa.ge/papers/information-security-an-effective-tool-for-sustainable-nigerian-national-security-and-development/

[10] A. A. Abubakar, J. Liu, and E. Gilliard, "An efficient blockchain-based approach to improve the accuracy of intrusion detection systems," *Electron. Lett.*, vol. 59, no. 18, p. e12888, 2023, doi: 10.1049/ell2.12888.

[11] K. V. Chitechi, B. Kiprono, and F. Tireito, "Cyber- Security Vulnerability and Initiatives in Kenyan County Governments," *Afr. J. Comput. Inf. Syst. AJCIS*, vol. 7, no. X, Art. no. X, Oct. 2023, doi: 10.1234/ajcis.v7iX.38.

[12] S. K. Fakunmoju, O. Banmore, A. Gbadamosi, and O. I. Okunbanjo, "Effect of Cryptocurrency Trading and Monetary Corrupt Practices on Nigerian Economic Performance," *Binus Bus. Rev.*, vol. 13, no. 1, Art. no. 1, Jan. 2022, doi: https://doi.org/10.21512/bbr.v13i1.7305.