Evaluating Nigeria's Readiness Against State-Sponsored Cyber Attacks: A Comparative Study of Cybersecurity Policies, Incident Response, and International Cooperation.

Abuh Ibrahim Sani[1], Ibrahim Yakub[2]

[1]Cybersecurity Analyst, EyBrids Ltd, United Kingdom, Email: saniabuh@gmail.com

[2]IT Auditor, Business service Organization, United Kingdom, Email:Ibrahim.yakub@hscni.net

Abstract

Nigeria's growing reliance on technology makes the country a prime target for state-sponsored cyberattacks. As cyberwarfare evolves, countries increasingly utilize cyber operations, posing threats to national security and economic stability. State-sponsored attacks targeting critical infrastructure can disrupt essential services. This paper evaluates Nigeria's readiness to defend against such attacks by examining cybersecurity policies, incident response capabilities, and international cooperation. Through a comparative analysis, the study identifies strengths and weaknesses of Nigeria's cybersecurity posture and offers recommendations for enhancing resilience against state-sponsored cyber threats. The role of international partnerships and capacity-building initiatives in bolstering Nigeria's cybersecurity defenses is discussed.

Keywords: Cybersecurity, cyberattack, Nigeria, State-sponsored, Policy

1. Introduction

The development of technology globalized the world, offering benefits in national security, economic development, and governance. State-sponsored cyberattacks threaten peaceful coexistence among nations (Johnson, 2024; Ishola et al., 2024). Nigeria's cybersecurity is a major concern due to cybercrime and insufficient security protocols. State-sponsored attacks are tools for economic sabotage and insecurity, often government-approved for political, economic, and military objectives. Understanding these motivations is crucial for prevention and response. These attacks pose a considerable threat to national security, economic stability, and public confidence. Nigeria's expanding digital economy attracts such attacks due to its strategic importance in Africa. This calls for decisive action to protect national security and critical infrastructure (Alabi, 2024).

State-sponsored cyber attacks have become tools used by many nations to cause economic sabotage and insecurity in some parts of the world (Azubuike, 2023). State-sponsored attacks are organized and well-founded activities, often approved by the government to achieve political, economic, and military objectives (Durojaye and Raji, 2022). Understanding the motivations underlying state-sponsored cyberattacks is crucial for formulating successful

measures for their prevention and response (Azubuike, 2023). The motivations for these attacks encompass political, economic, and military agendas. These attacks pose a considerable threat to national security, economic stability, and public confidence. Nigeria's rapidly expanding digital economy is increasingly attracting such attacks because of its strategic importance to African's economic development and political stability. The growing concerns called for a holistic approach for all policymakers across the world, especially Nigeria, to decisively act to prevent disasters to national security and critical infrastructure (Akoto, 2022).

As Africa's largest economy and digital leader, Nigeria adopts technologies like drones, AI, blockchain, IoT, 5G, introducing vulnerabilities in critical infrastructure and military operations. Increased global reliance on cyberspace has intensified state-sponsored cyber warfare. Nigeria's preparedness remains uncertain. (Allen, 2021). These technological developments also introduce vulnerabilities in critical infrastructure, military operations, and battlefield strategies, necessitating robust cybersecurity policies and incident response mechanisms (Azubuike, 2023). The growing global reliance on cyberspace has intensified state-sponsored cyber warfare, with powerful nations employing cyber operations as instruments of coercion and disruption (Familoni and Shoetan, 2024). While global trends reported increased reliance on cyber warfare, Nigeria's preparedness against state-sponsored cyber threats remains uncertain (Ishola et al., 2024).

Recent reports indicate a surge in state-sponsored cyberattacks, with China, Russia, Iran, and North Korea as primary perpetrators. Nigeria, like many African countries, is susceptible due to deficient frameworks, limited incident response, and inadequate international collaboration. Past incidents on financial institutions highlight the need for enhanced defenses (Azubuike, 2023).

Purpose of the Study

This research evaluates Nigeria's cybersecurity policies, incident response strategies, and international cooperation in mitigating state-sponsored cyber threats. It aims to:

- Assess Nigeria's readiness to counter sophisticated cyber threats.
- Conduct a comparative analysis of Nigeria's cybersecurity framework with global best practices.
- Propose recommendations for strengthening national cybersecurity and national security

2. Literature Review

2.1. State-Sponsored Cyberattacks

State-sponsored attacks are government-attributed cyber actions. They differ from cybercrimes in sophistication, resources, and intent to disrupt national infrastructure or cause

political tension. Nation-states leverage cyber capabilities for strategic, economic, and military objectives, using techniques like zero-day exploits, ransomware, phishing, and social engineering (Akoto, 2022). State-sponsored cyberattacks differ from conventional cybercrimes due to the level of sophistication, resources, and strategic intent to disrupt national infrastructure, steal sensitive information, or cause political tension (Baranovska et al., 2024).

State-sponsored cyber operations are increasingly part of hybrid warfare, blurring lines between conventional conflict and digital aggression (Oruc, 2020). Strong cybersecurity policies are needed to mitigate risks, especially in countries like Nigeria. Cyber risks endanger government data, enable cyberterrorism, and facilitate financial fraud, impacting national security. Cybersecurity flaws also hinder e-commerce and foreign investment (Azubuike, 2023). This evolution requires strong cybersecurity policies to reduce risks, especially for countries like Nigeria, which encounter increasing cyber dangers with fast digitization. Cyber risks put government data at risk, allow cyberterrorism, and facilitate financial fraud, they have a direct influence on national security (Sule et al., 2021). Additionally, cybersecurity flaws impede the expansion of e-commerce and deter foreign investment, which hinders the digital economy (Ferguson, 2024).

2.2. Cybersecurity Policies and Frameworks

Cybersecurity policies are foundational for national defense. Global frameworks like NIST, the EU's NIS Directive, and Singapore's Cybersecurity Act emphasize risk management, public-private collaboration, and incident reporting. Lack of regulation and consensus among nation-states poses risks (McGuire, 2021). Many African nations lack harmonized legal frameworks for cross-border cybercrimes, making infrastructure vulnerable. Nigeria's 2021 NCPS aims to align with international norms but faces enforcement challenges (Bouke et al., 2023) . It indicates that we may be at significantly higher risk from the internet than previously anticipated. Disparities in policy implementation persist, especially in developing countries posing the biggest threats to national security.

Alabi (2024) asserts that weak cybersecurity measures, limited infrastructure, and a lack of awareness and compliance with regulations, including the Cybercrime Act 2015, have contributed to the prevalence of cybercrime in Nigeria(Ibrahim et al., 2024). Lack of compliance and policy implementation may ultimately jeopardize the nation's key infrastructure to the actions of state-sponsored entities (Ukwandu et al., 2023). Analysis by Azubuike (2023) suggests that countries with centralized cybersecurity agencies, such as Israel's National Cyber Directorate, demonstrate higher reliance and underscore the need for Nigeria to strengthen governance structures.

Nigeria must expand cybersecurity training, improve international cooperation, exploit new technology, bolster policy enforcement, and raise cybersecurity spending in order to solve

these problems. Nigeria's economic stability and digital future depend on bolstering cybersecurity resilience.

2.3 Nigeria's Cybersecurity Landscape

Nigeria's cybersecurity reflects progress and vulnerabilities. Being Africa's largest digital economy, it faces increased cyberattacks, including phishing on government agencies and financial institutions (Interpol, 2023). Rapid digitization increases vulnerability, impacting the digital economy and national security. Ransomware, phishing, and disinformation increased during the 2023 elections, exposing infrastructure weaknesses. Economic challenges have increased financial crimes and insider threats (Sule et al., 2021). According to Delliote (2024) assessment, ransomware, phishing, and disinformation were among the cyber events that increased during the general elections in 2023, exposing weaknesses in vital infrastructure. Financial crimes linked to cyberspace have increased as a result of economic challenges, which have also increased insider threats.

Regulatory frameworks like the Nigeria Data Protection Act (2023) and the Cybercrime Act (2015) exist, but insufficient investments and lax enforcement exacerbate vulnerabilities. Emerging threats include AI-powered attacks and 5G risks. The 2015 Cybercrimes Act and NCC-CSIRT are steps forward, but many Nigerian organizations lack incident response plans and use outdated protocols. Legacy systems and low public awareness create vulnerabilities (Odumesi,2023). The environment is further complicated by emerging dangers, such as cyberattacks powered by AI and hazards associated with 5G.

Cyber threats are complex and evolving, posing risks to national security. Cybersecurity is critical for Nigeria's economy and national security. Cyber threats evolve with digitization, requiring proactive protection of national security and military operations.

3.Methodology

This research employs a qualitative methodology, primarily relying on the analysis of secondary data to evaluate Nigeria's readiness against state-sponsored cyberattacks. The study adopts a comparative approach, examining Nigeria's cybersecurity policies, incident response capabilities, and international cooperation mechanisms in relation to regional and global best practices. Some of the policy Documents use include analysis of Nigeria's National Cybersecurity Policy and Strategy (NCPS) 2021, the Cyber Crimes Act 2015, the Nigeria Data Protection Act 2023, and related amendments. Comparative analysis also such as policy documents from regional peers such as South Africa's Cybercrimes Act and Kenya's National Cybersecurity Strategy, and global models like the U.S. Cybersecurity and Infrastructure Security Agency (CISA) frameworks and the UK's National Cyber Security Centre (NCSC) strategies. Academic Articles and Research Papers: A comprehensive review of scholarly articles and research papers from reputable academic databases, journals, and publications focusing on cybersecurity, state-sponsored cyberattacks, and digital governance in Nigeria and globally.

4. Cybersecurity Policies

4.1. Review Nigeria's National Cybersecurity Policy and Strategy and legal frameworks

The Cyber Crimes Act of 2015 is the principal statute regulating cyber security in Nigeria. Its objective is to deter, detect, and prosecute cybercrime while safeguarding the nation's key infrastructure, electronic communications, and other digital assets (Nayak and Bello, 2024). The Act forbids several cybercrimes, such as identity theft, unlawful access, data theft, and cyberterrorism. Sanctions for these offenses vary from monetary fines to incarceration, contingent upon the gravity of the transgression. The legislation primarily addresses cybercrime, hence diminishing the necessity for a comprehensive cybersecurity statute that encompasses state-sponsored and all varieties of attacks (Alabi, 2024). Both documents aimed to guide initiatives for enhancing cyber-security capabilities to address threats arising from a multifaceted threat environment, including espionage and terrorism (Daniels, 2023).

The Office of the Nigerian National Security Adviser states that the National Cyber Security Strategy (NCSS) is the nation's preparedness framework designed to implement cohesive measures and strategic actions to ensure security and protection in cyberspace, safeguard critical information infrastructure, and cultivate a trusted cyber-community (Bukola, 2024). The Nigerian Communications Commission (NCC) and the Office of the National Security Adviser have formulated a National Cybersecurity Policy and Strategy. The Nigerian National Cybersecurity Policy and Strategy, formulated by the NCC and the National Security Adviser's Office, delineates the government's strategy for cybersecurity, highlighting the necessity for cooperation between the public and private sectors to devise and execute comprehensive cybersecurity protocols (Alabi, 2024).

The big question is, is Nigeria truly ready? Is the policy robust enough to protect cyberspace and critical infrastructure from cyber war? Our finding has identified some deficiencies in the cybersecurity policy in Nigeria which would be discussed in the next section. Amid various societal concerns, the issue of Cyber Security warrants paramount consideration. At present, cyber security concerns are increasingly attracting worldwide attention. Given its significance, policymakers, governments, and stakeholders must meticulously formulate guiding principles in the form of policies and plans to manage cyber security challenges (Daniels, 2023)

Nigeria's cyber-security policy has transitioned from an initial emphasis on combating cyber crime to a holistic approach encompassing national security, business interests, economic resilience, and community cyber safety concerns. Its military cyber policy is still in its nascent stages. Nigeria's dynamic technology start-up economy has robust innovative capabilities (Adisa, 2023).

The legal framework for cybersecurity in Nigeria is constantly changing to meet the current reality. with other measurements being suggested and evaluated. Additional relevant legislation encompasses:

1. ***Nigeria Data Protection Act 2023:*** *Building upon the NDPR, the Nigeria Data Protection Act was enacted on June 12, 2023. This Act establishes the Nigeria Data Protection Commission (NDPC), which is responsible for regulating the processing of personal information, promoting data processing practices that safeguard personal data security and privacy, and ensuring the rights of data subjects are protected. The Act strengthens the legal foundations of Nigeria's digital economy and facilitates the country's participation in regional and global economies through the trusted use of personal data.*
2. *Amendments to the Cybercrimes Act: In response to evolving cyber threats and concerns regarding the misuse of certain provisions, the Cybercrimes Act underwent amendments, culminating in the Cybercrime (Prohibition and Prevention) (Amendment) Act 2024, signed into law on February 28, 2024. These amendments aim to address criticisms related to the misuse of the Act and to strengthen measures against cybercrime.*

Interesting the amendment to section Section 21 of the Principal Act - Reporting, Cybersecurity Coordination, and Response Strengthens collaboration among cybersecurity organizations by requiring prompt reporting of cyber incidents to the National Computer Emergency Response Team (ngCERT) Coordination Center via sectoral CERTs or Security Operations Centres (SOC). The method guarantees cooperation and expedited incident reporting (Bukola, 2024)

The modification shortens the reporting timeframe for cyber incidents, including attacks and intrusions, from "7 days of its occurrence" to "72 hours of its detection," so enhancing the provision's operational impact. The clause has been criticized for being ineffective, as hacks may have transpired years before notice (Bukola, 2024). The diminished response time is essential for alleviating the effects of cyberattacks and protecting computer systems and networks. The amendment enhances cybersecurity measures and strengthens cyber resilience in both public and private sectors by stressing proactive reporting (Adeniran et al., 2024). Furthermore, the obligation to disclose disturbances that could impact other systems or networks aids in safeguarding vital infrastructure and key services from cyber threats.

To fulfil its cybersecurity goals, ONSA and ngCERT have executed many programs, like the National Cybersecurity Strategy, the Nigerian Internet Governance Forum, and the Cybersecurity Education and Awareness Programme (Alabi, 2024). These programs seek to improve cybersecurity governance, augment capabilities for preventing, detecting, and responding to cyber-attacks, and elevate cybersecurity as a national priority. Promote global cooperation and collaboration in cybersecurity (Damilola, 2024). Foster a proficient and

capable workforce in cybersecurity, Advocate for implementing best practices in cybersecurity and advance cybersecurity research and development (Ishola et al.,2024). Nonetheless, problems persist, including insufficient technical skills, inadequate response strategies, policy adherence, inadequate funds, corruption, and a deficiency of political will to enact improvements.

4.2 Compare Nigeria's policies with regional peers (South Africa's Cybercrimes Act, Kenya's National Cybersecurity Strategy) and global models (U.S. CISA, UK's NCSC)

The cybersecurity framework of Nigeria is based on the National Cybersecurity Policy and Strategy (NCPS) 2021, which delineates the nation's strategy for safeguarding its cyberspace (Nte et al., 2023). This strategy underscores a comprehensive and flexible framework, emphasizing collaboration among governmental bodies, the commercial sector, and individuals to protect digital ecosystems. The NCPS seeks to provide comprehensive legal and regulatory frameworks to combat cybercrime, safeguard critical infrastructure, and guarantee data privacy.

4.2.1 Comparison with Regional Counterparts

The Cybercrimes Act of South Africa aims to criminalize several cyber offenses, establish investigation protocols, and augment the capacity of law enforcement agencies. Nigeria and South Africa possess a notable digital presence and have had considerable cybercrime occurrences (Snail ka Mtuze and Musoni, 2023). Nigeria's NCPS offers a comprehensive strategic framework, whereas South Africa's strategy focuses on targeted legislative actions to address cybercrime (Nte et al., 2022).

Kenya's National Cybersecurity Strategy seeks to implement a coordinated framework for cybersecurity, emphasizing the protection of key infrastructure, capacity creation, and the enhancement of public awareness (Sang, 2022). A comparative analysis reveals that Nigeria and Kenya have established cybersecurity policies and strategies to address new risks and provide sustainable cybersecurity frameworks for Africa.

Table 1: Comparative Analysis of the cybersecurity policies, implementation strategies and enforcement mechanisms between Nigeria, South Africa, and Kenya

Aspect	Nigeria	South Africa	Kenya
Policy Framework	National Cybersecurity Policy and Strategy focus on addressing the cybersecurity challenges, enhance digital competitiveness and protect critical nation infrastructure and information	National Cybersecurity Policy Framework(NCPF) intended to coordinate cybersecurity efforts.	National cybersecurity strategy(2022) focuses on preventing cybercrimes, protecting critical infrastructure and promoting cybersecurity awareness.

Legislation	Cybercrimes(Prohibition, Prevention, etc.) Act (2015) criminalizes various cybersecurity crimes offenses and establishes legal frameworks for prosecution	Cybercrimes Act (2005) addresses cyber offenses but has been criticized for ineffectiveness and lack of comprehensive coverage	Computer misuse and cybercrimes Act(2018) provides a legal framework for addressing cybercrimes and establishes the national computer and cybercrimes coordination committee (NC4)
Implementation	Coordination efforts are fragmented despite existence of policies, practical implementation faces challenges due to lack of coordination among agencies.	Implementation of the NCPF has been slow with inadequate coordination among agencies and stakeholders.	The NC4 coordinate efforts has been great, but there is challenges in implementing strategies and ensuring effective collaboration among stakeholders.
Enforcement	Enforcement has been hindered by inadequate resources, lack of skilled personnel and insufficient public awareness.	Enforcement is weak due to slow policy implementation, lack of skilled labor and limited public engagement in cybersecurity practices.	Cybercrime remains prevalent, law enforcement requires enhanced knowledge and resources to effectively prosecute cyber offenses.
Public Awareness and Engagement	Lack of awareness is still an issues as authority are not convincing businesses and citizens to adopt best practices.	Public awareness campaigns are minimal. Difficulty in encouraging businesses and individuals to take proactive cybersecurity measures.	Some awareness programs are in place. However, broader public education and engagement are necessary to improve cybersecurity resilience
International Collaboration	Engages in regional cybersecurity initiatives.	Involved in continental efforts.	Collaborates with International Organization.

Source: (Nte et al., 2022)

From the table above shows that Nigeria, South Africa, and Kenya have established cybersecurity policies and legal frameworks, they face common challenges in implementation and enforcement, including coordination issues, resources constraints, and the need for

greater public awareness. Strengthening the gaps is very important to enhance their cybersecurity resilience against any form of threats.

4.2.2 Comparison with International Models

The Cybersecurity and Infrastructure Security Agency (CISA) spearheads the national initiative to comprehend, mitigate, and diminish risks to cyber and physical infrastructure. CISA underscores the importance of proactive defense plans, collaboration between public and private sectors, and robust regulatory frameworks (Onunka et al., 2023). This method differs from Nigeria's emphasis on establishing legal and regulatory frameworks, as indicated in the NCPS.

The National Cyber Security Centre (NCSC) offers guidance and assistance to both public and private sector entities, with the objective of enhancing the UK's cybersecurity framework (Nayak and Bello, 2024). The NCSC underscores the importance of proactive defensive methods and robust regulatory frameworks, similar to the methodology employed by CISA in the United States (UK). This proactive and cooperative strategy corresponds with Nigeria's focus on stakeholder coordination and international collaboration, as detailed in the NCPS. However, the lack of policy implementation and enforcement of the cybersecurity framework is a major problem facing the country and could create a vulnerability that could be exploited by threat actors. The US and UK are keen on policy implementation and monitoring whereas Nigeria is a major issue that needs to be addressed to strengthen the country's cybersecurity development. It’s not a formulated policy and framework but how effective are those structures to protect the data and critical national security.

5. Incident Response Capabilities

To combat the rising threat of state-sponsored cyber-attacks, Nigeria has significantly improved its cybersecurity system. Key to these initiatives is the creation of the Nigerian Computer Emergency Response Team (ngCERT), which acts as the national focal point for cybersecurity events. Notwithstanding this program, there are still difficulties in properly tracking and reacting to national cyber threats (Ikuero et al., 2022). The lack of a single database to track cybersecurity events and disseminate information causes scattered activity among several groups lacking effective coordination, which is a major problem. The National Cybersecurity Policy and Strategy (NCPS) was developed to address these gaps by supporting the establishment of the National Cybersecurity Coordination Centre (NCCC).

The National Cybersecurity Policy and Strategy (NCPS) was launched to solve these issues by supporting the establishment of the National Cybersecurity Coordination Centre (NCCC). The NCCC is meant to be the main body coordinating inter-agency and sectoral cybersecurity initiatives (Odumesi, 2023). As of March 2023, though, the NCCC had not been formed and cybersecurity duties were still spread over several institutions like the National Information Technology Development Agency (NITDA) and the Nigerian Communications Commission (NCC). The fast digital change, which has heightened susceptibility to cyber attacks and

threatens the economic stability and security of the country, adds more complexity to Nigeria's cybersecurity scene (Adisa, 2023). Inadequate legislative and regulatory frameworks, lack of cybersecurity awareness and training, and limited infrastructure all contribute to gaps that continue despite many policies and programs. Although Nigeria has established basic systems to fight state-sponsored cyber-attacks, coordination issues, infrastructure shortcomings, and lack of a coherent strategy undermine the efficacy of these efforts. Improving the country's resilience against advanced cyber threats depends on addressing these concerns (Bukola, 2024).

6. International cooperation

Nigeria signed the Budapest Convention on Cybercrime, but enforcement and participation are lacking. Real-time collaboration mechanisms are absent. Nigeria lacks an international threat intelligence center. Nigeria’s response procedures are largely domestic (Odumesi, 2023). International alliances with organizations like INTERPOL and ITU are crucial. Global best practices include monitoring, awareness initiatives, vulnerability management, and collaborative cyber defense. Nigeria needs to move from policy alignment to operational integration with global systems. The institutional capabilities and real-time collaborative mechanisms found in more developed countries are absent from Nigeria.

There are no established frameworks in Nigeria's cybersecurity ecosystem for exchanging threat intelligence in real time with international partners. Nigeria's capacity to successfully prevent or respond to cross-border assaults is limited since it does not yet have a similar international or regional threat intelligence center, in contrast to the UNICC's Common Secure Cyber Threat Intelligence platform, which facilitates joint defense across UN agencies. Cyberthreats including financial fraud, ransomware, and phishing frequently come from outside of Nigeria or are part of international criminal networks (Odumesi, 2023). Nigeria's response procedures, however, are largely reactive and domestic in nature, with little incorporation into international cybersecurity efforts. Nigeria becomes isolated as a result, and its ability to fully handle global cyberthreats is weakened.

According to Sule et al. (2021), these collaborations can help nations like Nigeria who are struggling with a lack of resources and skilled laborers by facilitating technical support, collaborative research, capacity building, and common frameworks. Global best practices, as detailed in the UNICC study, include ongoing monitoring, user awareness initiatives, vulnerability management, and collaborative cyber defense infrastructure (UNICC, 2023). By collaborating more with international organizations and funding agencies to build cyber resilience, Nigeria can modify these strategies.

7. Recommendations

For Nigeria to have a robust cybersecurity strategies to prevent against state-sponsored cyber-attacks, we recommends the following should be considered to strengthen her security architecture.

1. Establish and operationalize the National cybersecurity coordination centre (NCCC) as a matter of priority: Nigeria must expertise the full establishment of and operationalization of the NCCC. This requires a dedicated budgetary allocation, clearly defined governance structures, and the development of standardized inter-agency collaboration protocols.
2. Enhanced cybersecurity capacity building and training: Nigeria should implement a comprehensive national cybersecurity capacity building and training program targeting government personnel, critical infrastructure operators, law enforcement agencies, and the general public. This approach would improve the ability to prevent, detect, and respond to cyber threats, including state-sponsored attacks.
3. Strengthen Legal and Regulatory Framework and Enforcement: It is important to strengthen the legal and regulatory frameworks related to cybersecurity with a focus on effective enforcement and alignment with international best practices. Effective enforcement is essential to ensure compliance and accountability.
4. Foster Proactive Threat Intelligence Sharing and Collaboration: Implementing mechanisms for proactive threat intelligence sharing and collaboration is very important for quick detection, prevention and effective response to cyber-attack.
5. Improving Protection of Critical National Infrastructure: Its is important for a nation to prioritize the enhancement of cybersecurity measures for the protection of critical national infrastructure (CNI) sectors such as energy, telecommunication, finance and transportation.

8. Conclusion

The implementation of a cybersecurity strategy is crucial for attaining safe and secure cyberspace objectives in Nigeria. The Federal Government of Nigeria (FGN) formulated its cybersecurity policy and strategy to promote economic prosperity via digitalization. This policy, when executed by the specified strategy to mitigate cyber threats in Nigeria, will assist stakeholders in comprehending the security of their computer networks, enhance the coordination of cyber activities, and guarantee adherence to security standards, foster a more secure and resilient cyberspace, and effectively convey security measures, such as advisories, to stakeholders. The Office of the National Security Adviser (ONSA) is the governmental entity tasked with coordinating cybersecurity initiatives in Nigeria.

Cybersecurity in Nigeria is still mostly hampered by ineffective implementation, enforcement, and awareness training. A poorly organized method to cybersecurity leaves the nation open to cyberattacks endangering national security, vital infrastructure, and economic stability. The government must act aggressively to implement a thorough cybersecurity system. This will

guarantee the safeguarding of sensitive information, help to reduce risks, and improve national defense against cyberattacks. The constantly changing digital environment also depends much on international cooperation. Nigeria may gain from the sharing of essential information, best practices, and threat intelligence by encouraging alliances with other countries and worldwide cybersecurity groups. Apart from improving the cybersecurity strength of the nation, our collaboration will help to create a more secure digital environment for people, government agencies, and companies.

Reference

[1] Adisa, O.T., 2023. The impact of cybercrime and cybersecurity on Nigeria's national security.

[2] Adeniran, A.A., Adeniran, A.O., Familusi, O.B. and Adedayo, O., 2024. The Outlook of Cyber Security in African Businesses: Issues and Way-Out. *Management analytics and social insights*, *1*(2), pp.260-271.

[3] Alabi, M., 2024. Literature Review on Cybersecurity in Nigeria. *Available at SSRN 4818514*.

[4] Allen, N. (2021) Africa's evolving cyber threats. Available at: https://africacenter.org/spotlight/africa-evolving-cyber-threats/ (Accessed: 04/02/2025)

[5] Akoto, W., 2021. International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. Journal of Peace Research, 58(5), pp.1083-1097.

[6] AZUBUIKE, C.F., 2023. Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks. Nnamdi Azikiwe Journal of Political Science, 8(3), pp.101-114.

[7] Baranovska, T., Savitskyi, V., Serbov, M., Stoliar, Y. and Krutik, Y., 2024. The Impact of Cybercrime on State and Institutional Security: Analysis of Threats and Potential Protection Measures. *Economic Affairs*, *69*, pp.33-42.

[8] Bouke, M.A., Abdullah, A., ALshatebi, S.H., Atigh, H.E. and Cengiz, K., 2023. African union convention on cyber security and personal data protection: challenges and future directions. *arXiv preprint arXiv:2307.01966*.

[9] Bukola. A, 2024. Nigeria Cybercrimes (Prohibition, Prevention, etc.) Act Amendment: Charting Future Direction. https://www.techhiveadvisory.africa/insights/nigeria-cybercrimes-prohibition-prevention-etc-act-amendment-charting-future-direction?utm_source=chatgpt.com [Accessed Online, 2025]

[10] Daniels, O., 2023. *National Cybersecurity Policy and Strategy of Nigeria: A Case Study* (Doctoral dissertation, Capitol Technology University).

[11] Damilola, O., 2024. CYBER SECURITY AWARENESS IN DEVELOPING COUNTRIES IN AFRICA: LESSONS FROM NIGERIA.

[12] Delliote. (2024). Nigeria Cybersecurity Outlook.

[13] Durojaye, Henry, and Oluwaukola Raji. "Impact of State and State Sponsored Actors on the Cyber Environment and the Future of Critical Infrastructure." *arXiv preprint arXiv:2212.08036* (2022).

[14] Familoni, B.T. and Shoetan, P.O., 2024. Cybersecurity in the financial sector: a comparative analysis of the USA and Nigeria. *Computer Science & IT Research Journal*, *5*(4), pp.850-877.

[15] Ferguson, O. (2024). Cybersecurity and IT Governance Challenges in Nigeria: Strategic Investment Needs and the Path Forward for a Resilient Digital Economy. International Journal of Computer Applications, 0975-8887

[16] Ibrahim, Y.A., Ishaya, A.O., Yusuf, M., Nancy, I., Bijik, H.A. and Aiyedogbon, S.F., 2024, April. Cybersecurity and cybercrimes in Nigeria: An overview of challenges and prospects. In *2024*

[17] INTERPOL., 2023. *African Cyberthreat Assessment Report 2023: Cyberthreat Trends*. (Accessed: 05/02/2025)

[18] Ishola, H.S., Salawu Ibrahim, O. and Oyewole, L.E., 2024. SECURITY AND ITS SOCIO-ECONOMIC EFFECT ON NIGERIA NATIONAL INTEGRITY. [Accessed, 2025)

[19] Ikuero, F.E. and Zeng, W., 2022. Improving cybersecurity incidents reporting in Nigeria: micro and small enterprises perspectives. *Nigerian Journal of Technology*, *41*(3), pp.512-520.

[20] JOHNSON, M.O., 2024. Globalization and transfer of technology: The implications for Nigeria's economic development. *International Journal of Public Administration Studies*, *4*(1), pp.32-41.

[21] McGuire, M., 2021. Nation states, cyberconflict and the web of profit. *Hg. v. HP Threat Research. Online verfügbar unter https://threatresearch. ext. hp. com/web-of-profit-nation-state-report*.

[21] NAYAK, S.K. and BELLO, A., 2024. EVALUATING THE EFFECTIVENESS AND GAPS IN NIGERIA'S GOVERNMENT CYBERSECURITY POLICIES: RECOMMENDATIONS FOR ENHANCING CYBERSECURITY MEASURES. *Journal of Systematic and Modern Science Research*.

[22] Nte, N.D., Enoke, B.K. and Teru, V.A., 2022. A comparative analysis of cyber security laws and policies in Nigeria and South Africa. *Law Research Review Quarterly*, *8*(2), pp.233-258.

[23] Odumesi, J. (2023.) Cyber Threat Landscape in Nigeria. Cybersecurity Education Initiatives.

[24] Oluwawemimo, E., 2024. The Role of Artificial Intelligence in Incident Response for Digital Domain SMEs.

[25] Onunka, O., Alabi, A.M., Okafor, C.M., Obiki-Osafiele, A.N., Onunka, T. and Daraojimba, C., 2023. Cybersecurity in US and Nigeria banking and financial institutions: review and assessing risks and economic impacts. *Advances in Management*, *1*.

[26] Oruc, A., 2020, October. Claims of state-sponsored cyberattack in the maritime industry. In *Conference Proceedings of INEC*.

[27] Sang, M., An Appraisal of Kenya's National Cybersecurity Strategy 2022: A Comparative Perspective By: Michael Sang.

[28] Snail ka Mtuze, S. and Musoni, M., 2023. An overview of cybercrime law in South Africa. *International Cybersecurity Law Review*, *4*(3), pp.299-323.

[29] Sule, B., Sambo, U., Yahaya, M. A., & Mat, B. (2021). Cybersecurity and Cybercrime in Nigeria: The implications on National Security and Digital Economy. Journal of Intelligence and Cyber Security.

[30] Ukwandu, E., Okafor, E.N., Ikerionwu, C., Olebara, C. and Ugwu, C., 2023, March. Assessing cyber-security readiness of Nigeria to industry 4.0. In *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science 2022; 20–21 June; Wales* (pp. 355-374). Singapore: Springer Nature Singapore.

[31] UK, G., 2022. *National cyber strategy 2022* [online]