*Nigerian Journal of Technology (NIJOTECH)*
*Vol. 41, No. 3, May, 2022, pp.521-526*
*www.nijotech.com*

*Print ISSN: 0331-8443*
*Electronic ISSN: 2467-8821*
*http://dx.doi.org/10.4314/njt.v41i3.11*

# Preliminary Review of Cybersecurity Coordination in Nigeria

F. E. Ikuero

*Nigeria Computer Emergency Response Team, Abuja, NIGERIA*

**Abstract**
*Cyberspace presents significant opportunities that enhance communication, and boost business and socio-economic prosperity in Nigeria. While cyber criminals thrive to exploit any vulnerability for their gains, the Nigeria Government has taken some measures to safeguard its cyberspace. This study evaluates the efforts of the Nigeria Government in the coordination of cybersecurity in the country. It used secondary source methodology by reviewing previous and related research works including books, articles among others. The study found that Nigeria has established a national Computer Emergency Response Team (CERT) and four active Sectoral Computer Security Incident Response Teams (CSIRTs). It also revealed that the Nigeria Government through the Office of the National Security Adviser (ONSA) formulated the National Cybersecurity Policy and Strategy (NCPS). It was found that the establishment of the National Cybersecurity Coordination Centre (NCCC) would enhance the implementation of cybersecurity programs in Nigeria. Amongst others, the study recommended that the ONSA should facilitate the approval for the establishment of NCCC.*

**Keywords:** Cybersecurity, Cybersecurity policy implementation, Cybersecurity sensitization, Office of the National Security Adviser

## 1.0 INTRODUCTION

The economic losses that nations, organizations, and other users of cyberspace incurred due to cyber-attacks threaten every government of nations worldwide. Attacks are a major cause of socio-political problems worldwide [1]. Nations count their losses to cyber-attacks, such as business shut down and payment of Ransom to cyber criminals [2] [3, 4]. As technology advances, cybersecurity needs to evolve in order to mitigate its threats being a serious concern to cybersecurity managers in every country of the world [5, 6]. When countries, companies, and users of cyberspace consistently experience attacks, it poses a setback to the national security, economy, and development [6]. Additionally, as the ease of accessing and using cyberspace grows the menace of cybercrime increases [7]. Some of these crimes include business email compromise; social media account hijack, and impersonation, cyber espionage, malware, Distributed Denial of Service, advance fee fraud, phishing, and Ponzi schemes amongst others. Therefore, it is important for governments of nations to understand that any negligence or partial interest in cybersecurity could have severe harmful implications on the functionality of its entire system. Nigeria's cyberspace is experiencing an increase in digital transformation [8]. The majority of the day-to-day activities including social interactions, business transactions, security, and law enforcement operations amongst others, have now embraced the use of the Internet.

Therefore, cyberspace has become a valuable and indispensable determining factor of socio-economic prosperity, national security, and development. However, the growth of cyberspace has expanded the span of cybersecurity threats. Cyber threats are now more detrimental to individuals, businesses, organisations, government functions and critical infrastructure across the country cyberspace compare to the times when the internet was still at the developmental stage. According to [9], Nigeria state lost approximately NGN127 Billion to cyber-attacks on a yearly basis. Apart from financial losses, nations, organizations, and individuals could experience scarcity of products, unavailability of services, chaos, and loss of trust among others in the event of cyber-attacks. The foregoing suggests the need for the Federal Government of Nigeria (FGN) to continually ensure adequate protection of its cyber domain. Consequently, the aim of this study is to evaluate the activities of the Nigeria Government in the coordination of cybersecurity across the nation's cyberspace and thereafter make recommendations.

The subsequent part of this paper is structured as follows: Section 2 is the literature review while Section 3 discusses related works. Section 4 elucidates the challenges and Section 5 highlights the way forward. Section 6 is the recommendation while Section 7 concludes the paper.

*Corresponding author **(Tel:** +234 (0) 8057725360**)**
**Email address:** fikuero@cert.gov.ng (F. E. Ikuero)

## 2.0 LITERATURE REVIEW

Cybersecurity is a process of safeguarding nations, organizations, individuals, and users' information and communication technology assets as well as Critical National Information Infrastructure (CNII) by identifying and responding to the threats that could compromise the data that are stored or transmitted via the systems [10].

Cybersecurity is aimed at protecting information and data from disclosure to unauthorized users, protecting data from modification, and making services (information and data) accessible to authorized users at all times [11, 12]. It is a condition achieved when the confidentiality, integrity, and availability of information systems, networks, and data are safeguarded when attacks occur [13]. Therefore, it is a condition that protects users' information infrastructure from threats.

Cybersecurity sensitization connotes the process of engaging relevant stakeholders in order to expose them to current activities trending in cyberspace with a view to educating them on the requisite actions that will secure individual, organizational, or users' Information and Communication Technology (ICT) devices in their custody. It is planned to engage stakeholders to understand the prevailing cyber threats, tactics, and operations of cyber criminals [14]. The awareness level and the actions required by computer users plus compliance will determine the extent to which attacks on computer networks and systems would be prevented [14, 15]. Cybersecurity sensitization is usually organized for a specified audience considering the medium of communication that would be most effective. Channels of conducting cybersecurity campaigns include webinars, Jingles, flyers, billboards, posters, face-to-face workshops, and conferences. Nowadays, organizations, as well as sectors, leverage the internet to conduct their transactions; thereby serving as a tool that enables them to contribute to national and social-economic development. This makes sensitization on cybersecurity for employees and users a vital requirement [16].

Cybersecurity policy implementation is one of the standard practices that enable nations to achieve safe and secure cyberspace objectives. Among other reasons, the FGN developed its cybersecurity policy and strategy to enhance business prosperity via digitalization [17-22]. A policy that is implemented in accordance with the outlined strategy would:

a. Reduce threats in cyberspace.
b. Enable relevant stakeholders to understand the security posture of their computer networks.
c. Enable cyber activities to be coordinated in an efficient manner.
d. Enforce security programs according to standards.
e. Ensure compliance.
f. Effectively communicates security measures such as advisories to stakeholders.

ONSA is responsible for cybersecurity coordination efforts in Nigeria. Up until 2015 when ngCERT was established, cybersecurity activities were fully handled by ONSA. With the rise of Internet Service Providers (ISPs) in the country, following the deregulation of the telecommunications sector in Nigeria, accessing the internet became easy. As individuals and organizations employ the internet for carrying out their daily activities, fraudsters leveraged it for committing cybercrimes [23]. These criminal activities necessitated the Federal Government of Nigeria (FGN) to constitute a presidential committee domiciled in ONSA to investigate the activities of these fraudsters in the nation's cyberspace in 2003. Cybersecurity efforts of ONSA shall be highlighted subsequently.

### *2.1 National Cybersecurity Initiative*

The presidential committee proposed the National Cybersecurity Initiative (NCI) in 2003, saddled with the responsibilities to:

a. Enlighten the Nigerian public on the nature and threat of cybercrime.
b. Build capacity across Security and Law Enforcement Agencies (SLEAs) to extend statutory functions on cybercrime related issues.
c. Establish a technical and legal framework that will secure computer systems as well as protect the nation's Critical Information Infrastructure.
d. Create a platform for Public-Private- Partnership to set standards and guidelines for Nigeria's cybersecurity.
e. Build international law enforcement cooperation to enhance Nigeria's effort in combating cybercrime.

### *2.2 Nigeria Cybercrime Working Group*

In 2004, the Federal Government established the Nigeria Cybercrime Working Group (NCWG) to sustain the objectives of NCI. NCWG consisted of officials drawn from Ministries, Departments, and Law Enforcement Agencies. NCWG amongst other activities conducted enlightenment on cybercrime in public and private institutions across Nigeria [18].

### *2.3 Directorate of Cybersecurity*

Furthermore, in 2006, the FGN through ONSA created the Directorate of Cybersecurity (DOC) to uphold the work of NCWG and coordinate cybersecurity activities in the country [18]. In this regard, the group was mandated to implement the objectives of NCI as follows:

a. Establish and develop a framework for National Computer Emergency Response Team
b. Establish collaboration with CERTs globally.
c. Establish a National Digital Forensic Laboratory, and coordinate the training of SLEAs in Nigeria and their utilization of the facility.
d. Conduct sensitization campaign for Non-Governmental Organizations.
e. Sponsor passage of the Computer Security and Critical Information Infrastructure Protection Bill in Nigeria's National Assembly.

### *2.4 The Cybercrime Act of 2015*

Nigeria's National Assembly enacted the Cybercrime Act in 2015. Amongst others, the objectives of the Act are to:

a. Provide an effective regulatory and institutional framework for preventing cybercrimes in Nigeria.
b. Ensure the protection of CNII.
c. Promote cybersecurity Promote the protection of computer systems.

### *2.5 National Cybersecurity Policy and Strategy*

The NCPS was initially developed in 2014, in line with Section 41(1b) of the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015. The 2014 version of the NCPS was reviewed in 2021. The policy document is intended to ensure the formulation and effective implementation of an all-inclusive cybersecurity framework for Nigeria. It is a document that provides a roadmap and action plan for enhancing Nigeria's security posture in cyberspace.

### *2.6 Nigeria Computer Emergency Response Team*

Section 41(c) of the Cybercrime Act of 2015 established the ngCERT domiciled in ONSA [19]. It is the apex office responsible for managing cybersecurity activities in Nigeria. The establishment of ngCERT in 2015, enhanced cybersecurity in Nigeria's cyberspace as it received collaboration from both local and international stakeholders. The ngCERT has the mandate to monitor the Nigerian Cyberspace and respond to Cybersecurity incidents [19]. For effective cybersecurity coordination, the Nigeria government is adopting the Sector-based approach.

Consequently, ngCERT serves as the coordinating and regulatory body for the operation of sector-based Computer Security Incidents Response Teams (CSIRTS) in Nigeria as stipulated in NCPS 2021. Currently, the functional Sectoral CSIRTs in Nigeria include those belonging to the National Information Technology Development Agency, Defence Space Administration, and National Communication Commission. Figure 1 illustrates the relationship between the various coordinating stakeholders in Nigeria cyber ecosystem.

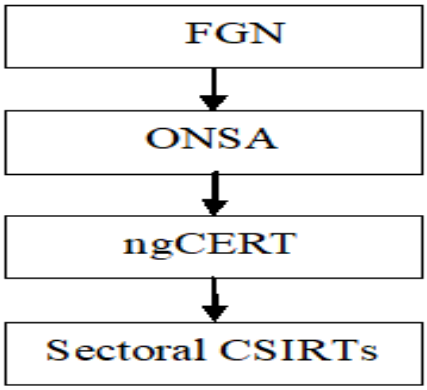


**Figure 1:** The coordinating stakeholders in Nigeria cyber ecosystem

### *2.7 Cybercrime Advisory Council*

The Cybercrime Advisory Council (CAC) is mandated vide Section 43 of the Cybercrime Act 201 to provide strategic direction and functions for cybersecurity policymakers in Nigeria. The CAC is to facilitate the implementation of Nigeria's cybersecurity program [19, 20].

## 3.0 RELATED WORKS

In [21], the researchers asserted that the current policy and strategy effort of the FGN in solving cybersecurity concerns has not satisfactorily mitigated the challenges threatening its cyberspace. According to [10], the study opined that Nigeria has developed policy and strategy for combating cybersecurity threats but organizations, general populace and users do not implement the strategy due to inadequate sensitization.

Sensitization exposes users to the knowledge of dangers associated with cyber threats; thereby making them to comply with the strategies outlined to implement the policy instead of ignoring it. In [22], the writer argued that the knowledge gained could enable stakeholders defend themselves when attack occurs. It is in this regard that ONSA and ngCERT organized a Sector-based sensitization workshops for implementing NCPS 2021 under seven groups including telecommunication, education, power, oil and Gas amongst others held from September to December 2021. However, there is need for ONSA and ngCERT to consider extending the sensitization workshop on the implementation of the NCPS 2021 to other sectors that were not included in the September to December 2021 program.

In [7], the authors stated that several challenges are facing Nigeria in its quest to ensure data security in its cyberspace; thus delaying the pace at which incidents would be investigated and mitigated. The researchers identified

cyber threat intelligence as a major hindrance to effective mitigation. Consequently, they suggested strategic policies for cyber analysis in order to maintain data security.

According to [10], cybercrimes take place globally but exploitation of vulnerabilities and national impacts differ from one nation to another depending on their commitment level. In [23], the writer opined that Nigeria's commitment to combating cybercrime is rated medium; therefore, urged the FGN and all relevant cybersecurity stakeholders to strengthen their efforts in curbing cybercrimes.

## 4.0 CHALLENGES

The technological sophistication with the associated malicious intent of cyber criminals poses huge challenges to the nation's cyberspace and internet users despite the coordination efforts of the Nigeria Government [6]. Some of the challenges of cybersecurity coordination are explained below:

### *4.1 Absence of National Cybersecurity Coordination Centre*

The NCCC is to be domiciled under the existing structure of ONSA in line with the provisions of the Cybercrimes (Provision, Prevention Etc) Act, 2015, and the NCPS 2021 as well as with global best practices [19, 20]. However, NCCC, among other tasks shall be responsible for handling the implementation of all cybersecurity initiatives and programs designed for ensuring progressive use of the nation's cyber domain. While some of these programs and initiatives have been successfully completed by the ngCERT, others are still in view as ngCERT may not have the requisite authority to discharge such mandates; therefore, slowing down the implementation of cybersecurity programs that would better secure Nigeria's cyberspace and guarantee national security and prosperity.

### *4.2 Lack of Adequate Cybersecurity Skill-sets*

The capacity for investigating and prosecuting cybercrimes on digital evidence by SLEAs is insufficient [7]. Therefore poses a huge challenge in promoting cybersecurity in Nigeria [5]. This deficit exists across all the relevant SLEAs from the investigators to the prosecutors.

### *4.3 Absence of Cybersecurity Research, Development and Innovation Centre*

Currently, Nigeria lacks the harmonization of research, development, and innovation efforts in its cybersecurity ecosystem. This militates against safe cyberspace in Nigeria [5]. Thus synchronizes the efforts of stakeholders including incubation centers, global community, academia, government, and private research institutions.

### *4.4 Inadequate Cybersecurity Awareness*

Inadequate cybersecurity awareness of computer users constitutes a high threat to Nigeria's cyberspace. Computers and other ICT infrastructure require protection against unauthorized access and incompetent users [22]. However, Nigeria is yet to achieve a remarkable awareness level.

## 5.0 WAY FORWARD

The factors required for addressing the challenges of cybersecurity coordination in Nigeria are stated as follows:

### *5.1 Establishment of the National Cybersecurity Coordination Centre*

In order to ensure that Nigeria completely utilise the benefits of cyberspace while mitigating every associated threat, it became necessary to effectively harmonise the cybersecurity efforts of every relevant stakeholder within the Nigeria cyber ecosystem. This informed the need for establishing the NCCC, which shall be the Nigeria cybersecurity coordinating body. The Centre will adopt a whole-of-society inclusiveness approach to implement Nigeria's National Cybersecurity Programme in line with extant laws. In view of this, it is necessary that ONSA could consider intensifying efforts in facilitating the approval for the establishment of NCCC.

### *5.2 Cybersecurity Skill-sets Development*

To proffer a solution to the challenges of inadequate skill-sets, the CPS 2021 provides for the establishment of the National Cybersecurity Training Institute (NCTI) to oversee capacity building as well as regulate the certification of cybersecurity experts in the country. However, the NCTI is yet to be established. Accordingly, it is important that ngCERT and ONSA facilitate the establishment of the NCTI for the realisation of the objective of adequate skill-sets.

### *5.3 Creating Cybersecurity Research, Development and Innovation Centre*

In order to sustain secure cyberspace, there is the need to harmonise cybersecurity research, development, and innovation efforts. For effective harmonisation, it is necessary to create a centre that would develop frameworks for promoting indigenous cybersecurity technologies such as solutions and applications. To achieve this, ONSA, ngCERT relevant Ministries, Department and Agencies may consider facilitating the establishment of an RDI centre.

### *5.4 Improved Cybersecurity Awareness*

Cyber threats particularly those associated with fraud need both technical protection and awareness of cyber hygiene for users of the internet. Cyber criminals exploit any vulnerability such as errors caused by users. Raising the awareness level of cybersecurity in Nigeria would enable more internet users to acquaint themselves with actions and inactions that could expose their computers to being vulnerable to attacks. In view of the foregoing, it is needful for ONSA and ngCERT to extend cybersecurity sensitisation across all sectors and regions of Nigeria.

## 6.0 RECOMMENDATIONS

In view of the foregoing, below are the recommendations that could improve cybersecurity coordination in Nigeria:

a. ONSA should facilitate the approval for the establishment of NCCC.
b. NCCC should ensure the establishment of NCTI for adequate skill-sets development.
c. The ngCERT and relevant stakeholders should the establishment of RDI centre.
d. ONSA and ngCERT should extend cybersecurity sensitisation across all sectors and regions of Nigeria.

## 7.0 CONCLUSION

Cybersecurity incidents experienced in Nigeria's cyberspace have made the Government through ONSA and ngCERT emplace actionable measures that would forestall threats in its cyber domain. Implementation of these measures would ensure efficient coordination that would reduce cybersecurity incidents in its cyberspace. So far the FGN has enacted the Cybercrime Act of 2015 and formulated NCPS. The absence of NCCC to serve as a cybersecurity coordinating body, inadequate cybersecurity skill-sets, lack of RDI centre, and inadequate cybersecurity awareness were identified as challenges to cybersecurity coordination in Nigeria. Accordingly, the establishment of the NCCC, the development of Skill-sets, the creation of an RDI centre, and improved cybersecurity awareness were highlighted as the way forward. Consequently, the study highlighted recommendations including the establishment of NCCC and cybersecurity across the board amongst others.

## REFERENCES

[1] Udanor, C.N., Ogbodo, I.A., Ezugwu, O.A. and Ugwuishiwu, C.H. "A Logistic Predictive Model for Determining the Prevalent Mode of Financial Cybercrime in Sub-Saharan Africa''. *In The International Conference on Emerging Applications and Technologies for Industry*, Springer, Cham, 4, 2020, pp. 137-151.

[2] Hunter, B. ''til the Next Zero-Day Comes: Ransomware, Countermeasures, and the Risks They Pose to Safety'', *Safety-Critical Systems eJournal*, 1(1), 2022.

[3] Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F. and Materne, S. "Cyber risk and cybersecurity: a systematic review of data availability'', *The Geneva Papers on Risk and Insurance-Issues and Practice*, 2022, pp 1-39.

[4] Van Camp, C. and Peeters, W. "A World without Satellite Data as a Result of a Global Cyber-Attack'' *Space Policy*, 59, 2022, pp 101458.

[5] Oyelere, S.S., Sajoh, D.I., Malgwi, Y.M. and Oyelere, L.S. November. "Cybersecurity issues on web-based systems in Nigeria: M-learning case study''. *In 2015 International Conference on Cyberspace , CYBER-Abuja, Institute of Electrical and Electronics Engineers*, 2015, pp. 259-264.

[6] Garba, A. A., Siraj, M. M., Othman, S. H. and Musa, M. A. "A Study on Cybersecurity Awareness among Students in Yobe State University, Nigeria: A Quantitative Approach'' *International Journal on Emerging Technologies*, 2020, 11(5), pp. 41–49.

[7] Saidu, I.R., Suleiman, T. and Akpan, U.E. "The Challenges of Security Threat in Nigeria Cyberspace'' *Fudma Journal of Sciences*, 5(1), 2021, pp 193-201.

[8] Idowu OA. "Cybercrimes and Challenges of Cyber-Security in Nigeria'', *Wukari Journal of Sociology and Development*, 2021.

[9] Awhefeada, U.V. and Bernice, O.O. "Appraising the Laws Governing the Control of Cybercrime in Nigeria'', *Journal of Law and Criminal Justice*, 8(1), 2020, pp 30-49.

[10] Garba, A.A. and Bade, A.M. "The Current State of Cybersecurity Readiness in Nigeria organizations'', *Educational Research (IJMCER)*, 3(1), 2021, pp 154-162.

[11] Odumesi, J.O. "A socio-technological analysis of cybercrime and cyber security in Nigeria'' *International Journal of Sociology and Anthropology*, 6 (3), 2014, pp 116 – 125.

[12] Frank, I. and Odunayo, E. (2013) "Approach to cyber security issues in Nigeria: challenges and solution'',

*International Journal of Cognitive Research in science, engineering and education*, 1(1), 2013, pp100-110.

[13] Kaur, G., Habibi Lashkari, Z. and Habibi Lashkari, A. "Introduction to Cybersecurity. In Understanding Cybersecurity Management in FinTech'', *Springer Cham*, 2021, pp 17-34.

[14] Moturi, C.A., Abdulrahim, N.R. and Orwa, D.O. "Towards adequate cybersecurity risk management in SMEs'' *International Journal of Business Continuity and Risk Management*, 11(4), 2021, pp.343-366.

[15] Trim, P.R. and Lee, Y.I. "The role of B2B marketers in increasing cyber security awareness and influencing behavioural change'' *Industrial Marketing Management*, 83, 2019, pp 224-238.

[16] Zamsuri, A., Syafitri, W. and Pane, E.S. "Evaluation of Information Security Awareness on Digital Marketing (Case Study of MSME in Indonesia)'', *Advances in Humanities and Contemporary Studies*, 2021, 2(1), pp 192-210.

[17] Sunkpho, J., Ramjan, S. and Ottamakorn, C. "Cybersecurity policy in ASEAN countries''. *In 17th Annual Security Conference*, March, 2018, pp. 1-7.

[18] Quarshie, H.O. and Martin-Odoom, A. (2012) "Fighting cybercrime in Africa'' *Computer Science and Engineering*, 2(6), 2012, pp 98-100.

[19] Cybercrimes, Prohibition and Prevention Act, 2015, https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf. Accessed 20 April 2022.

[20] National Cybersecurity Strategy and Policy, 2021. https://www.cert.gov.ng/ngcert/resources/national_cybersecurity_policy_and_strategy_2021.pdf. Accessed 20 April 2022.

[21] Calderaro, A. and Craig, A.J. "Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building'' *Third World Quarterly*, 41(6), 2020, pp 917-938.

[22] Garba, A.A. "Cybersecurity Awareness of University Students in Nigeria'' *Analysis Approach. Turkish Journal of Computer and Mathematics Education (TURCOMAT)*,12(12), 2021, pp 3739-3752.

[23] Akinyetun, T.S. "Poverty, Cybercrime and National Security in Nigeria'', *Journal of Contemporary Sociological Issues*, 1(2), 2021, pp1-23.