

INFORMATION SECURITY: AN EFFECTIVE TOOL FOR SUSTAINABLE NIGERIAN NATIONAL SECURITY AND DEVELOPMENT

Aliyu Ahmed Abubakar, Department of Computer Science, Kaduna State University, Kaduna, Nigeria
School of Cyberscience and Engineering, Wuhan University, Wuhan, China Corresponding
Adamu Umaru Shamsuddeen, Department of Computer Science, Kaduna State University, Kaduna, Nigeria
School of Cyberscience and Engineering, Wuhan University,

ABSTRACT: Information security is the exercise of protecting information by means of mitigating information threats and risks by averting or decreasing the probability of inappropriate or unauthorized access to data, or the unlawful usage, exposure, disruption, erasure, corruption, alteration, assessment, recording, or devaluation of information. It similarly encompasses actions planned to decrease the adversarial effects of such incidents. Information security's prime goal is the protection of the integrity, confidentiality, and availability of data for efficient policy implementation, and without obstructing the productivity and development of the organization. An effective information security strategy would be the best measure to adopt to tackle the insecurity challenges faced by Nigeria which as well obstructs its potential to drive sustainable national security and development. This study defines those effective information security measures and strategies to be adopted as a tool to attain the desired said information security goal. This paper concludes that these measures and strategies will be effective for sustainable Nigerian national security and development. Nevertheless, this study provides recommendations that will enhance sustainable Nigerian national development by adopting these information security measures.

KEYWORDS: *Information Security, Cyber Security, National Security, National Development, Information Security Strategy*

1. INTRODUCTION

The global security environment is constantly changing with an evolving landscape of threats (Świątkowska, 2017). Various countries are suffering from one security challenge to another ranging from war, terrorism, cyber terrorism and theft, arm banditry, kidnapping for ransom, blackmail, coup, civil unrest, etc. This makes information security and assurance more in need than ever as a countermeasure to most of the security challenges. Countries that are victims of such security concerns need a more sophisticated information security strategy for sustainable national development. Africa specifically is occupied with such security concerns led by countries such as Mali, CAR, Libya, and Sudan with Nigeria as the nerve centre due to dreaded insurgents such as Boko Haram and the Islamic States West Africa Province (ISWAP). The problem here according to Paul (2022) is that most African militaries are ineffective because most African countries lack a strong sense of national identity. An important and critical threat among the Eko (2022) five threats to national security is cybersecurity. Others are hostile governments, terrorism, proliferation, and national disaster & diseases.

Since the Iraqi war, the Saudi Arabian government has embarked on a course of political, economic, and social reform that reflects a growing understanding by the royal family members, technocrats, and businessmen that Saudi Arabia must reform and diversify its economy and create vast numbers of new jobs for its growing population which has yielded results (Anthony, 2005). On June 10, 2021, the Standing Committee of China's National People's Congress passed the Data Security Law (DSL), which took effect on September 1, 2021. The major drive of the DSL is to regulate data activities, safeguard data security, promote data development and usage, protect individuals and entities' legitimate rights and interests, and safeguard state sovereignty, state security, and development interests (Latham & Watkins, 2021). The DSL, together with the Network Security

Law and the proposed Personal Information Protection Law, formed an increasingly comprehensive legal framework for information and data security in the People's Republic of China (PRC). As the protection of ICT infrastructure is in Switzerland's national interest, the Swiss Federal Council commissioned the national strategy for the protection of Switzerland against cyber risks pursuing the early identification of threats and dangers in the cyber field, improvement of the resilience of critical infrastructure and effective reduction of cyber risks, especially cybercrime and cyber sabotage (National strategy for the protection of Switzerland against cyber risks, 2012). The formation of a joint task force for cyber security and the building of a National Cyber Command Center that will be the go-to centre for cyber security in Nigeria, facilitate the integration for all cyber intelligence in all governmental parastatals and other institutions in Nigeria and also collaboration among stakeholders is a recommended measure in reforming information security in Nigeria (Tope, 2016).

2. RELATED CONCEPT

2.1 Nigerian National Security

National security also called national defence is the security and defence of a sovereign nation including its citizens, economy, and institutions which is observed as the obligation of the government. National Security as documented by President Obasanjo's regime in 2002 is the aggregation of the security interest of all individuals, communities, ethnic groups, political entities and institutions in the territory of Nigeria (Saleh & Émile, 2018). Components of national security such as military security, socio-political security, information security, energy security, food security, environmental security, health security, education system security, etc. must be utterly collaborated and improved to achieve sustainable national development (Rasim, Yadigar, Rasim, & Aliguliyev, 2021).

The approach of the Nigerian government towards national security remains unsatisfactory according to Chinecherem & Paullregbenu (2015) hence, conducted research examining the security challenges facing the Nigerian government and their implications for national stability. Among the recommendations of the research is the provision of better information security measures. Sahel security at the Tony Blair Institute, USA, has reported that there are five (5) security challenges bedevilling Nigeria. They are; Jihadism, Farmers-Herders clashes, Banditry and Kidnapping, Separatist agitation, and Oil militants (Aliyu, 2021). According to United Nations, by the end of 2020, conflict with Boko Haram alone has led to the death of about 350,000 people and forced millions out of their homes while another splinter group called the ISWAP has emerged in recent years (Aliyu). ISWAP has allied and surpassed Boko Haram with strong resistance to the Nigerian military and this has become a distinct threat to Nigeria's national security.

The Nigerian national security strategy (2019) has defined some key security concerns of the nation for which policies and strategies to implement them have been articulated depending on other national strategic policies such as the National Counter Terrorism Strategy, Cybersecurity Policy and Strategy, the National Defence Policy and the Economic Recovery and Growth Plan. Conversely, the security situation has persisted.

2.2 Information Security

Statistically, all over the world and since 2006, there has been a form of cybercrime committed daily (Yakubu, 2017). Nigerian cyber criminals are daily formulating different methods of committing this form of crime and the existing methods of trailing these criminals are no longer suitable to deal with their new tricks. Tope (2016) has conducted research he called Cyberharam: Can Nigeria Prepare For The Next Generation Of Terrorists where he explained that in confronting the challenges posed by cyber threats, one major deliberation is to identify our critical infrastructure and evaluate the risks to these systems so as to identify threats and vulnerabilities. Examples of the said critical infrastructure include those supporting our financial and telecommunication

systems, and systems hosting classified national security information amongst others. At the conclusion of the assessment, a long-term roadmap that will guide investments in securing our infrastructure should be set.

Another area of concern is cloud security as many governments today host their data on the cloud. A number of security threats associated with cloud data services, not only cover traditional security threats, e.g., network eavesdropping, illegal invasion, and denial of service attacks, but also includes specific cloud computing threats, e.g., side-channel attacks, virtualization vulnerabilities, and abuse of cloud services have been a serious area of concern in terms of information security (Ahmed, 2020).

2.3 National Development

National development is the capability of a country to raise the standard of living of its citizens. It can be accomplished by providing individuals with basic livelihood requirements such as security, food, health, and education, and also supplying them with employment. The Nigerian national development plan is a bridge for the country's long-term plan currently being developed, that is, National Development Plan 2021-2025 Olanrewaju (2021) and Nigeria Agenda 2050 with vision to make Nigeria a country that has unlocked its potential in all sectors of the economy for a sustainable, holistic, and inclusive national development (Ariyo-Dare, 2020).

3. INFORMATION SECURITY STRATEGY

Developing an effective information security strategy and taking steps to ensure compliance is a critical step to avert and mitigate security breaches. To make the security strategy justly effective, one needs to update it in response to changes in Nigeria. New threats, conclusions drawn from previous breaches, and other changes to the information security posture should be observed (Orion, 2019). Also make the information security policy practical and enforceable

with an exception system in place to accommodate requirements and urgencies that arise from different parts of Nigeria. It's also vital to differentiate between Information Security and Cyber Security strategies and policies. The National Institute of Standards and Technology (2022) defines information security as the "protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability." The institute defines cyber security as the "ability to defend or protect the use of cyberspace from cyber-attacks." Notably, the difference is in the scope.

4. CONCLUSION AND RECOMMENDATIONS

The Nigerian government needs an effective information security strategy as the best measure to deploy so as to tackle the insecurity challenges faced by the country which as well obstructs its potential to drive sustainable national security and development. There are many advantages of enhancing information security such as having a secure national identity database, nurturing good governance, improving the physical security of citizens, encouraging economic development, fostering confidence among citizens established on the security and transparency it provides, and eventually reinforcing democracy (Sixtus, 2021). Therefore, the recommendations of this study which revolve around the three basic principles of information security; confidentiality, integrity, and availability can be stated as follow:

1. The Nigerian Government should increase its efforts towards the enhancement of capturing and registering citizens and foreigners through the National Identity Management Commission (NIMC); NIMC should enhance its collaboration with databased government parastatals and private organizations

such as INEC for voters cards, Banks for BVN, the Nigerian police, military, customs, immigration service for international passport, federal road safety corps for vehicle registration and drivers licence, all telecom companies for sim cards, all basic, secondary and tertiary institutions, examination bodies such as NECO, JAMB, WAEC NBAIS, and NAPTEP to construct a mega data pool using the National Identification Number (NIN) as the Nigerian social security number. NIN registration is still faulty due to internal challenges such as lack of power, tribalism, religion, illiteracy, scammers, and lacks of clear benefits definition attached (Sixtus, 2021).

2. Another recommendation is the full adoption of the Global Position System (GPS) and Closed-Circuit Television (CCTV) for tracing known and unknown armed bandits,

Kidnappers, and other terrorist organizations across the country. It is also recommended to sensitize and monitor social media and messaging applications such as Facebook, Twitter, and Whatsapp.

3. The Nigerian government should boost the Information and Communication Technology (ICT) sector as It is believed that ICT has the potential to help Nigerians develop various skills including entrepreneurial skills, research and academic skills, economic and management skills, political skills, etc., which have become a potent force in transforming social, economic and political life globally (Emmanuel, Eneh, Isaac, Arinze, & Ahmed, 2021).
4. Building a go-to information security centre that will collaborate with all security and intelligence agencies with other related and relevant government parastatals.

REFERENCES:

- 1) Ahmed, A. A. (2020). Improving Cloud Data Security by hybridization of ZeroKnowledge Proof and Time-Based One-Time Password. *KASU JOURNAL OF MATHEMATICAL SCIENCES*, 116-126.
- 2) Aliyu, T. (2021, July 19). *Nigeria's security crises-five different threats*. Retrieved from BBC News website: www.bbc.com
- 3) Anthony, H. C. (2005). *National Security in Saudi Arabia: Threats, Responses, and Challenges*. Riyadh: <https://www.csis.org/analysis/national-security-saudi-arabia>.
- 4) Ariyo-Dare, A. (2020, July 13). *Agenda 2050: A new thinking with citizen participation and inclusion*. Retrieved from Vanguard Website: <https://www.vanguardngr.com/2020/07/agenda-2050-a-new-thinking-with-citizen-participation-and-inclusion/>
- 5) Chinecherem, U., & Paullregbenu, P. (2015). *Security Challenges and Implications to National Stability*. Anambra : Project: Child Labour and Its Determinants in Informal Sector of Onitsha.
- 6) Eko, O. (2022, 03 10). *five threats to national security and how the government protects its citizens* . Retrieved from Safetymanagement.eku.edu: Safetymanagement.eku.edu
- 7) Emmanuel, I. T., Eneh, A. H., Isaac, S., Arinze, U. C., & Ahmed, A. A. (2021). ICTs - An Efficient Tools for Entrepreneurs Amongst the Nigerian Youths. *Proceedings of the 27th SMART-iSTEAMS- IEEE, MINTT Conference Academic City University College* (pp. 267-272). Accra, Ghana: www.isteam.net/ghana2021.
- 8) Latham & Watkins. (2021, July 21). *China's New Data Security Law: What to Know*. Retrieved from LW website: <https://www.lw.com/thoughtLeadership/china-new-data-security-law-what-to-know>
- 9) *National strategy for the protection of Switzerland against cyber risks*. (2012, June 19). Retrieved from Enisa Website: [https://www.enisa.europa.eu/topics/national-cyber-security-](https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf)
- 10) [strategies/ncss-map/National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf](https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf)

- 11) NSS. (2019). *National Security Strategy*. Abuja: <https://ctc.gov.ng/wp-content/uploads/2020/03/ONSA-UPDATED.pdf>.
- 12) Olanrewaju, O. (2021, December 21). *As Nigeria Unveils National Development Plan 2021-2025, these are Twenty Key Points to Note*. Retrieved March 11, 2022, from Dataphyte Website: <https://www.dataphyte.com/latest-reports/economy/as-nigeria-unveils-national-development-plan-2021-2025-these-are-twenty-key-points-to-note/#:~:text=The%20National%20Development%20Plan%20targets,persons%20and%202025%2074.01%20persons>.
- 13) Orion, C. (2019, May 30). *The 8 Elements of an Information Security Policy*. Retrieved from Exabeam Website: <https://www.exabeam.com/information-security/information-security-policy/>
- 14) Paul, C. (2022, 03 10). *Security Threats Facing Africa and its Capacity to respond*. Retrieved from cco.ndu.edu: cco.ndu.edu
- 15) Rasim, M. A., Yadigar, N. I., Rasim, S. M., & Aliguliyev, R. M. (2021). Information Security as a National Security Component. *Information Security Journal: A Global Perspective*, 1.
- 16) Saleh, B., & Émile, O. (2018). NATIONAL SECURITY STRATEGY DEVELOPMENT: CASE STUDY NIGERIA. *Africa Center for Strategic Studies*.
- 17) SIXTUS, E. (2021, October). *Issues in national identity in the 21st century*. Retrieved from The Cable Website: <https://www.thecable.ng/issues-in-national-identity-in-the-21st-century>
- 18) Świątkowska, J. (2017). Cybersecurity Statecraft in Europe: A Case Study of Poland. *Georgetown Journal of International Affairs*, 84-94.
- 19) The National Institute of Standards and Technology. (2022, March 11). *COMPUTER SECURITY RESOURCE CENTER*. Retrieved from CSRC Website: <https://csrc.nist.gov/glossary/term/cybersecurity>
- 20) Tope, A. (2016). 'Cyberharam': Can Nigeria Prepare For The Next Generation Of Terrorists? *Deloitte Nigeria*. Retrieved March 11, 2022, from <https://www.mondaq.com/nigeria/terrorism-homeland-security-defence/533396/cyberharam39-can-nigeria-prepare-for-the-next-generation-of-terrorists>
- 21) Yakubu, A. M. (2017). Cyber Security Issues in Nigeria and Challenges. *International Journal of Advanced Research in Computer Science and Software Engineering*, 315.