International Journal of Advanced Research in Global Politics, Governance and Management | IJARGPGM
p-ISSN: 2636-686X | e-ISSN: 2636-6878
Volume 3, Number 1 September, 2022

The State and the Management of Cybersecurity in Nigeria

Kingsley Chigozie Udegbunam
Peace and Conflict Resolution Unit
School of General Studies, University of Nigeria, Nsukka

Article DOI: 10.48028/iiprds/ijargpgm.v3.i1.11

Abstract

This study investigated Nigeria's responses to the numerous threats in its cyberspace. The growth of information and communication technology, a consequence of the Fourth Industrial Revolution, has led to the emergence of new forms of security threat. As an emergent dominant global sphere, cyberspace serves as a platform for the advancement of socio-economic activities such as e-business and e-governance. However, criminal elements within and outside the state have also acquired the skills to invade and exploit cyberspace for subversive purposes and other personal gains. Consequently, the state bearing in mind the essence of the social contract, undertakes to ensure the security of this new domain by protecting its citizens' cyberspace and critical cyber infrastructures. This study, therefore, aims at interrogating how the Nigerian state has managed cybersecurity by asking if Nigeria's cybersecurity architecture efficiently prevent insecurity in Nigeria's cyberspace? In searching for answers to these questions, the study relied on primary and secondary data. The study drew its primary data from an online structured questionnaire administered through an online survey platform, *Monkey Survey* to185 respondents with cyberspace presence. Data from secondary sources were drawn from relevant national agencies with a mandate to operate in or about Nigeria's cyberspace as well as extant literature. Data sourced from the questionnaire were analysed using *Monkey Survey* statistical tools for analysis while data obtained via the secondary sources were subjected to content analysis. The finding shows that Nigeria's cybersecurity architecture does not efficiently prevent insecurity in its cyberspace. It further proposes a model for the management of cybersecurity in Nigeria.

Keywords: *State, Cybersecurity, cyber-crime, Cyberspace, Nigeria, Securitisation*

Corresponding Author: **Kingsley Chigozie Udegbunam**

Background to the Study

The term cybersecurity refers to a range of policies and actions aimed at making the cyberspace safe for useful transactions. The origin of the concept of cybersecurity is usually traced to scientists, especially those with bias in computer and telecommunication network who used the term to capture most of the risks of breached associated with networked computers in the 1990s (Nissenbaum 2005). The term however became popular among social scientists in the context of examining the social effects of digital technologies (Nissenbaum 2005). By the beginning of the first decade of the new millennium, cybersecurity has become a global concern due to the formidable nature of cyber threats. While the cyber space has greatly enhanced global socioeconomic activities, some states and non-state actors have also mastered its usage for the advancement of parochial interests and criminal activities.

Cyber-crimes refer to all criminal activities that are either dependent on the use of computers and related soft and/or hardware as well as crimes facilitated by computers, computer-related network and other ICT (McGuire & Samantha 2013). Like in most issues of vulnerability, developing states have also been most vulnerable to cyber-crimes due to a number of factors that include weak institutions. In addition to their vulnerability to cyber-crimes, these states also breed cyber criminals, who due to the borderless nature of cyberspace, constitute significant threats to global security, disrupting foreign relations, and puncturing the positive impacts of globalisation and technological advancement. As developing states with weak institutions, most criminally-minded African citizens are exploiting the cyberspace as a vehicle for international criminal activities. This is made possible by the increased access to the internet and many states' weak cyber security capability.

The last two decades have seen Africa witnessing rapid internet penetration and associated cyber challenges. From a mere population of about 4.5 million internet users in the year 2000, more than 526 million, representing 39.3 percent of Africa's 1.5 billion population, now have access to the internet (Internet World Stats, 2020). A 2018 report by Serianu, an Information Technology (IT) firm, shows that several African countries suffer heavy financial losses due to cyber-crimes and weak cyber governance. For instance, Nigeria lost $649 million while Kenya and Tanzania lost $210m and $99m respectively to cyber-criminal networks in 2018 (Kshetri, 2019). The cyberspace of all leading African economies such as Nigeria, South Africa, Egypt, Kenya, and others are constantly threatened by local and international cyber criminals.

Specifically, Nigeria remains a major source of global concern for cyber-criminal activities. As indicated by Chawki (2010) more than 50,000 people globally were victims of Nigerian cyber-criminal activities resulting in a loss of over $5 billion in the first decade of this surge. By the second decade, a cyber-criminal industry with local and international networks has emerged in Nigeria with cybersecurity agencies only recording little successes. The United States' Federal Bureau of Investigation (FBI) widely reported a burst of an international cyber-criminal network that supports the argument that Nigeria has become a major exporter of cyber criminals. The FBI indicted Obinwanne Okeke and 79 others for over $50 million internet frauds against American companies (FBI, 2019). Consequently, Nigeria's management of her cyberspace for the enhancement of national security requires a critical interrogation.

Problematique

The emergence of the internet has propelled the growth of global proximity by altering the way people interact concerning obtaining and sharing access to information, news and opinions. The International Telecommunication Union (ITU), as of 2017, estimated that there are over 3 billion internet users globally, corresponding to more than 45 per cent of the world population". By 2017, the population of internet users had increased to about 3.17 billion with the majority of the users from Asia, followed by Europe and North America. This figure is estimated to have grown by 30 per cent by the end of 2018.

This attendant growth has equally resulted in the emergence and growth of cyber threats. According to a 2016 report by Norton (2016), Cyber threats accounted for a loss of $388 billion in the global economy. Cybercriminals continued to breach networks with highly targeted attacks which increased from 10 to 18 per cent between 2014 and 2015. Incidences of cyber threats such as fraud, economic espionage, cyber terrorism, cyberwar and denial-of-service attacks have continued to portend security threats to many. The Global Cybersecurity Index (GCI) reports that from 2014-2018, the global economy lost $7.45 billion orchestrated by 1,509,679 cyber-attacks (GCI, 2019).

Like many other modern states, Nigeria is not immune to cyber-criminal activities and attacks that are capable of threatening national and societal security. The 2016 Telegraph report of cybersecurity mapping, shows that Nigeria ranked as the 28 most vulnerable country to cyber threats. Similarly, Business Journal (2019) reported that Nigeria ranked 3rd in the world's most mobile malware attacked nation. Many institutions, including financial and telecommunications, have continued to suffer huge monetary losses as a result of cyber war declared on the nation by certain criminal elements in the society. This has implications for people security. The vulnerability of cyberspace has allowed the invasion of cyber infrastructure and consequently leaving many citizens unprotected. It is against this backdrop that this study seeks to examine the state management of cybersecurity by interrogating Nigeria's cybersecurity architecture capacity to efficiently prevent insecurity in Nigeria's cyberspace.

Literature Review

A number of authors and researchers have paid attention to the menace of cybersecurity in Nigeria and elsewhere. Osho, Falaye and Shafi'I (2013) sought to highlight cyber tools and techniques used by terrorists in Nigeria in their activities, assess the government's response so far and capacity in tackling terrorism, and proffer recommendations that can help mitigate the menace. The authors reported that cyberspace could fast become the biggest promoter of terrorism in Nigeria and that unfortunately, the government does not possess the necessary cyber-capabilities to tackle this in the country. To forestall this, they highlighted the need to view the security of the country's cyberspace as the trigger point in developing effective anti- and counter-terrorism strategies, and consequently, put necessary cybersecurity measures in place to this effect. While this study is apt to the Nigerian situation, it is narrow because it limited the cyber threats to just cyber terrorism thereby excluding other formidable threats to national security.

Olayemi (2014) investigated the management of cyber-crime and cyber threats by Nigerian security agencies. Using a mixed-method, the study identified the legal challenges faced by government security agencies in enhancing cybersecurity. Olayemi (2014) contended that the Advance Fee Fraud Act of 2006, Money Laundering Act of 2004, the Economic and Financial Crime Commission Act of 2005, and the evidence Act of 1948 are not sufficient legal instruments to combat insecurity in Nigeria. The author argued that inadequate legislation, the absence of a national internet gateway for Nigeria, lack of a national framework and infrastructure for the protection and management of electronic payment fraud are key challenges to the security agencies in the management of cybersecurity in Nigeria.

Saulawa and Abubaka (2014) focused on cyber-crimes in Nigeria, the examples of cyber-crimes and also an overview of the cyber-crimes Act 2013. They argued that cyber-crime associated with Nigeria include email scams, phishing and credit card fraud; Nigerian banks are susceptible to these attacks. They further opined that it is evident that many Nigerians, organisations and government are investing a significant amount of money in the protection of their ICT systems and networks. They argued that some organisations only fight cyber-crimes through cybersecurity experts only when security is breached or compromised. They contend that the recent cyber-crimes Act established by the Nigerian legislation intends to fight cyber-crimes from all angles. They held that the Cyber Crime Act is a roadmap in curbing the menace of cyber-crime in Nigeria. This study adopted a legal perspective to examining cyber-crimes in Nigeria. While this enhances our understanding of the impact of the Cyber Crime Act on cybersecurity, it is the case that legal perspective is only reactionary and not defensive as in cyber warfare. The point, therefore, is that the study considers only legal provision in just cyber-crime thereby excluding combative efforts of all forms of warfare on Nigerian cyberspace.

Osho and Onoja (2015) compared the contents and structure of the NCSPSN with that of countries such as the UK, US, Canada, the Netherlands, Japan, Kenya, and France. The authors argued that the comparative analysis with similar documents of selected countries was reflective of the fact that the documents are reasonably comprehensive in terms of content. The evaluation based on the harmonized frameworks also showed that the required contents expected to be typically contained in such documents are largely present. The authors however, contended that certain aspects which appear to be critical to the Nigerian scenario such as an explanation of the current national cyber security state, partnership with internet service providers, establishment of digital identity frameworks, and the development of a military cyber defense capability were seen to either be utterly absent or only barely implied. The study is no doubt relevant to the concern of cyber warfare as an aspect of cybersecurity management in Nigeria.

Jack and Ene (2016) argued that the internet revolution and the advent of mobile telephone technology in Nigeria have posed unintended risks to the society, as evident in increasing surge in cyber-crime such as yahoo-yahoo-advanced fee fraud, hacking, cyber stalking, virus attacks, espionage, character defamation, pornography, online gambling and so on. The authors concluded that widespread cyber-crime hurts the socio-economic development of Nigeria as it tarnishes the image of the country at a global scale, deters foreign investments, and reduces confidence in the digital economy; with huge financial losses to individuals, business organisations and the government. Following these submissions, they proposed that the Nigerian government should enact comprehensive laws to curb cyber-crime while building the capacity of security experts on contemporary cybersecurity technology.

Sawanah (2018) contended that the thriving and escalating cyber-crime on Sierra Leonean cyberspace is a function of the weakness of the state legal infrastructures and poor cybersecurity architecture. This is compounded by very little knowledge about cybersecurity among the working class of Sierra Leone. The author further argued that the absence of strong laws against cyber insecurity has impeded the capacity of the security agencies to secure Sierra Leonean cyberspace. Supporting Sawanah's view, Bancila (2018) opined that the state is the lead actor in the security of cyberspace through the provisions of legal frameworks. This responsibility becomes more urgent as a consequence of the fact that by 2020 about 50 billion devices were projected to be connected to the Internet (Gartner 2017) thereby increasing the possibility of more vulnerability and cyber insecurity.

Still in search of an appropriate response to the cyber insecurity, Robinson, Jones, Janicke, and Maglaras (2018) borrowed from the concept and practice of peacekeeping, as applied to traditional warfare, to suggest an adaptation of the principles of the United Nations peace support operations such as peacemaking, peacebuilding, peacekeeping and peace-enforcement to the management of cybersecurity especially inter-state or international cyber warfare. In a separate but similar study, Robinson, Jones, Janicke, and Maglaras (2018) proposed cyber observation, monitoring and reporting (OMR) as critical cybersecurity infrastructure that should be mainstreamed into any cybersecurity architecture. Their study x-rayed the practicality of OMR as an integral part of cyber peacekeeping. Consequently, OMR is seen as key elements of any cybersecurity architecture.

No doubt the emergence of cyber threats has also necessitated the examination of the phenomenon by scholars and other authors. As seen in the literature reviewed, most studies have concentrated on the nature of cyber threats, with descriptive analysis of typologies as well as the responses from organisations and governments. However, while descriptive studies on the nature of cyber threats in Nigeria exist, specific interrogation of the state responses is limited. Examining the state cyber architectures and assessing their effectiveness using empirical data is lacking in extant studies. In-depth study of state responses, such as would be undertaken in this work, is the foundation for appropriate theorization of functional and adequate management of cyber threats in Nigeria. Current literature has left this largely unexplored and the very few studies on state management of the cyberspace narrow their scope to reactive actions of the state security agencies thereby reducing the issue to mere descriptive studies.

Materials and Method

The population of this study comprises people with access to the internet in Nigeria. According to the Nigerian Communication Commission (NCC), there are about 108,500, 000 Nigerians with access to the internet as of May 2019 (Udegbunam, Akale & Eshilama, 2021). Out of this population, the focus is on those who are active users of the internet such as persons with, at least one email address, conduct online financial and social activities through online media.

Data for this study were sources through documentary method and survey method. Therefore, the secondary data for this study will be obtained from official documents of the federal and state security outfits such as the Nigerian Financial Intelligence Unit (NFIU), Special Control Unit against Money Laundering, National Information Technology Development Agency (NITDA) and Economic and Financial Crimes Commission (EFCC).In addition to official documents, this study will equally make use of other secondary data sources such as books, journal articles, conference papers, periodicals, and other written works. Thus, primary data for this study were collected through online structured questionnaires administered through the Monkey Survey.

Content analysis and quantitative methods of data analysis such as frequencies and percentages, means and standard deviations, charts and graphs were adopted for the presentation and interpretation of results for the study. On the other hand, the study also adopted quantitative data analysis techniques such as simple descriptive analysis, frequency tables, charts and graphs to analyse data collected through the structured questionnaires. To do this, responses from the questionnaires using Monkey Survey tools for analysis and Microsoft Excel. Hence, a combination of content analysis and quantitative analysis enabled us to test the assumptions of the study.

Table 1: Logical data framework

Research topic	Research questions	Hypothesis	Major variables of the hypothesis independent (X) Dependent (Y)	Empirical Indicators of Variables	Source of Data	Method of Data Collection	Method of Data Analysis
The state and the management of cybersecurity in Nigeria	Does Nigeria's cybersecurity architecture efficiently prevent insecurity in Nigeria's cyberspace?	Nigeria's cybersecurity architecture enhances the management of cybersecurity	(X) The efficiency of Nigeria's cyberspace security architecture	1) Effective laws, rules and regulation guiding cyberspace. 2) Special units created in the different security agencies for monitoring cyberspace 3) Effective legal framework for prosecuting cyber-crimes	Primary (questionnaires) and Secondary Source (Text books, journals, conference papers, seminar papers and official documents).	Documentary and Online Survey Methods of data collection (Monkey Survey)	Content analysis and Percentage
			(Y) The management of cybersecurity	1) Securitised cyberspace 2) Dissemination of information concerning cyberspace 3) Arrest and trials of cyber criminals			

Results, Findings and Analysis

Respondents Demography

Figure 1: Respondents' Occupation

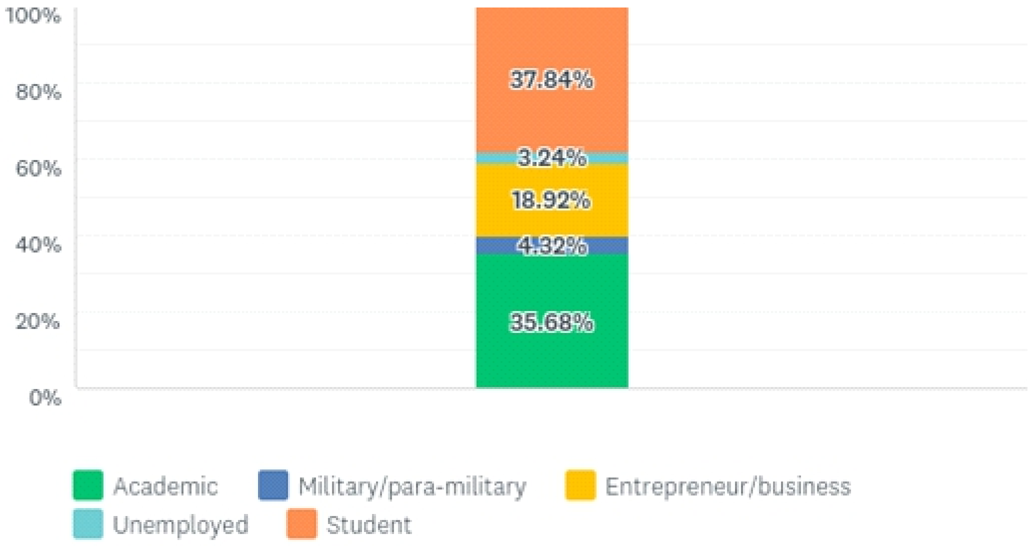
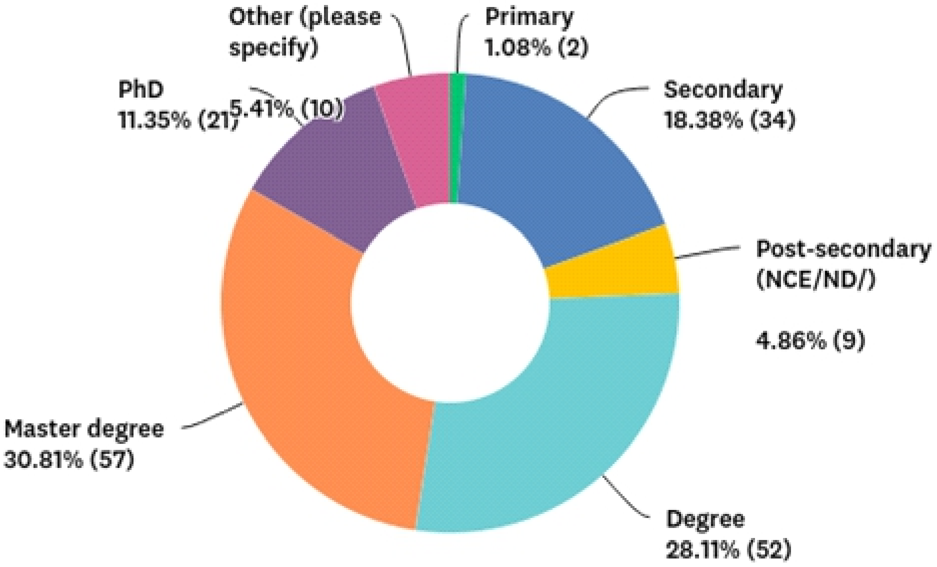


Figure 2: Respondents' Highest Academic Qualifications



Source: Researcher Fieldwork (2020)

Nigeria's Cyber Security Architecture and Prevention of Insecurity in Nigeria's Cyberspace

The major aim of this section is to analyse current legal and institutional architecture for the management of cybersecurity in Nigeria to also identify provisions relevant to fighting these acts or omissions and the lapses of the institutional and legal regime, whether or not they are effective in fighting cyber-crime in Nigeria and relevant in international cooperation against cyber-crime. Put differently, this section examines the nexus between cyber-security architecture and the prevention of cyberspace crimes.

Cyber Security Laws and the Protection of Nigeria's Cyber Space

With the increase in cyber-crimes in Nigeria, given that the fundamental duty of any state is to provide maximum security that will ensure the well-being of its citizenry, the Nigerian state and its relevant institutions have passed laws prohibiting cyber-crimes and prescribing punishment for offenders. Some of the laws include but not restricted to the following, EFCC Act; the Criminal Code Act, the Penal Code Act, the Anti-Terrorism Act, the Advance Fee Fraud Act, the National Cyber Security Strategy (NCSS), 2014, and the cyber-crime Act, 2015. Yet incidences of cyber-crimes have persisted in Nigeria. The Institute for Security Studies (2020) states thus:

In 2018, commercial banks in Nigeria lost a cumulative N15 billion (US$39 million) to electronic fraud and cybercrime. This was a 537% increase on the N2.37 billion loss recorded in 2017. Over 17 600 bank customers and depositors lost N1.9 billion to cyber fraud in 2018, with fraud rising by 55% from the previous year.

No doubt, the high rate of cyber-crimes in Nigeria has created for Nigeria a notorious image among the comity of nations. These laws were put together at different times and with different objectives and purpose. However, a common and unifying thread among them is that they have curbing cyber-crimes as part of but not their sole objectives. In sum, the essence of these various laws is to fight cyber-crimes in Nigeria. Table 2 below gives a better view of the relevant laws passed by the Nigerian state to tackle cyber-crimes in Nigeria.

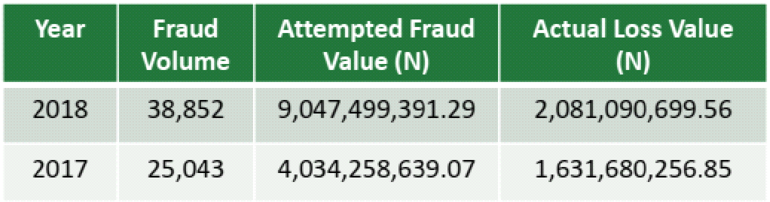
Table 2: Laws, Acts and Regulations against Cyber Crimes in Nigeria

S/N	Names of the Laws, Acts or Regulations	Year of Passage	Nature of cyber-crimes Fought
1	Economic and Financial Crimes Commission (the EFCC) Act	2002	All though none-specific but it covers a whole of crimes related to bank and financial transactions
2	Money Laundering (Prohibition) Act 2011 as amended in 2012	2011/2012	To safeguard the Nigerian Financial System.
3	The Criminal Code Act Cap.	2004	To trial and convict persons for criminal activities
4	Terrorism Prevention Act	2011	Track, monitor and prevent transactions that may relate to Terrorism or terrorist financing
5	National Cyber Security Strategy (NCSS)	2014	Provides general guidelines for cybersecurity management.
6	Cybersecurity Act	2015	Focuses on computer-related offences; Content-related offences; Computer integrity offences;

Source: Compiled by the Researcher (2020)

Table 1 above explicitly reveals some of the laws passed to fight cyber-crimes in Nigeria; when they were passed and the nature of their purpose. Although, these laws are worthwhile and have helped in fighting cyber-crimes in Nigeria the growth of cyber-crimes negates their very claims. Cases abound of persons that have been convicted or prosecuted as a result of these laws. Yet many cyber criminals are having a field day at their craft because of either poor or non-enforcement of these laws. For instance, many young Nigerians are now into cyber-crimes despite the existence and operations of these laws. The figure reveals the number of frauds committed and the actual amount of money lost.

Figure 3: Number of frauds committed through cyberspace in 2017/18 in Nigeria



Year	Fraud Volume	Attempted Fraud Value (N)	Actual Loss Value (N)
2018	38,852	9,047,499,391.29	2,081,090,699.56
2017	25,043	4,034,258,639.07	1,631,680,256.85

Sources: Enhancing Financial Innovation and Access, (2019)

From Figure 3 above, it can be seen that the number of cybercrimes in Nigeria has not reduced despite the presence of existing laws against them. From 25, 043 recorded cases in 2017 to 38,852 recorded cases in 2018 with a corresponding increase in the amount of money involved; from more than 1 billion in 2017 to over 2 billion in 2018. This shows that cybercrimes have not reduced in Nigeria in terms of volume and amount involved. The reasons might be due to how inefficient and effective the laws are.

Security Agencies and Arrest/Prosecution of Cyber-criminals

As shown in the above analysis, the Nigerian state has many agencies that are in the business of fighting cybercrimes. Part of their job or their full-time responsibilities is to arrest and prosecute persons involved in cybercrimes. They are vested with the powers and with the backings of the necessary laws creating them to combat cyber-crimes. These agencies or special units are charged with arresting and taking to the appropriate court of law those involved in cybercrimes to be tried and charged. They include but not restricted to Directorate for Cybersecurity (DfC), NFIU, Special Control Unit against Money Laundering, NITDA, the EFCC among others. The table below will give an overview of the various agencies involved in the fighting of cyber-crimes in Nigeria when they were created and some of their duties and arrest. It will help gauge their performance and understand their effectiveness.

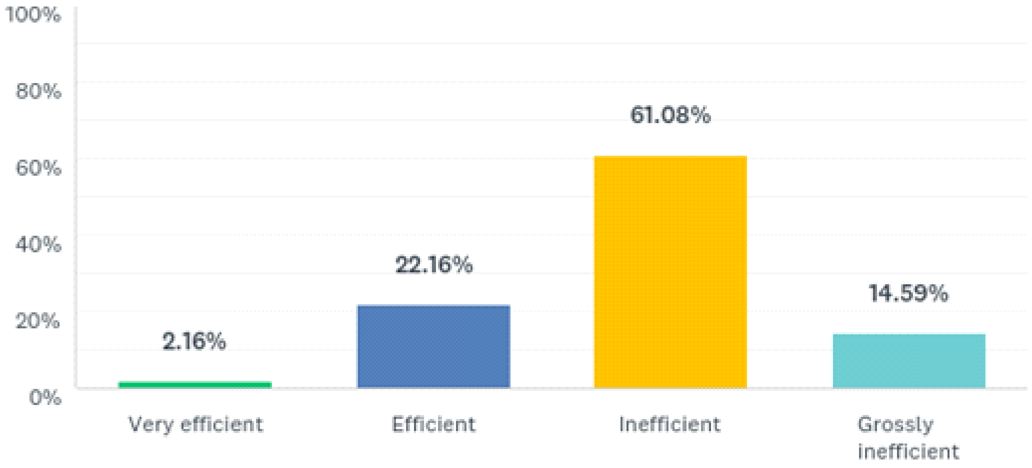
Table 3: Agencies Combating Cyber Crimes in Nigeria

S/N	Names of Agencies	Year of creation	Job Description
1	Economic and Financial Crimes Commission (Nigerian Financial Intelligence Unit, NFIU)	2004/2009	To safeguard the Nigerian Financial system and contribute to the global fight against money laundering, terrorism financing and related crimes through the provision of credible financial intelligence
2	The Special Control Unit against Money Laundering	2011	Has the responsibility under the provisions of the Money Laundering (Prohibition) Act No. 1, 2011 (as amended)19 to monitor, supervise and regulate the activities of Designated Non-Financial Businesses and Professions in Nigeria
3	National Information Technology Development Agency	2007	Create a framework for the planning, research, development, standardization, application, coordination, monitoring, evaluation and regulation of Information Technology practices, activities and systems in Nigeria
4	Directorate for Cybersecurity (DfC)	2015	Developing effective framework and interfaces for inter-agency collaboration on cyber-crime and cybersecurity; ii. Establishing appropriate platforms for public-private partnership (PPP) on cybersecurity; iii. Coordinating Nigeria's involvement in international cybersecurity

Source: Compiled by the author from Available literature

Table 3 above shows the existence of agencies that fight cyber-related crimes in Nigeria. Some of these agencies have tried, no doubt, in combating cyber-crimes in Nigeria. Despite their efforts, cyber-crimes remain unabated in Nigeria. It has not gone down. Rather evidence has shown a yearly increase in cyber-crimes in Nigeria. The functions of these agencies are all geared towards fighting against cyber-crimes. These agencies are saddled with the responsibility of fighting combating cyber-crimes. Yet a majority of the respondents in this study believe that many of the agencies have not fared well in the fight against cyber insecurity. The figure below shows the views.

Figure 4: How would you rate Nigeria's cybersecurity agencies



From Figure 4 above, many of the respondents agreed that most of the cyber-security agencies of the Nigerian state have not been efficient. Out of 185 respondents, 61.08% noted that cyber-security agencies in Nigeria are not doing well although, 22.16% argued otherwise, stating that they are efficient. However, a large number of the respondents have faulted their performance. These views cast a dark shadow over the affairs of these agencies. Nevertheless, it will not be fair not to list the achievements of some agencies in the fight against insecurity. This is because the Nigerian media are awash with the arrest and prosecution of persons with regards to cyber-crimes. Despite the negative views about their performance as expressed by the respondent in this study, these agencies, since their creation, have helped the Nigerian government in the prevention, investigation and prosecution of several offences relating to cyber-crimes. The Table 4 below reveals a timeline of Nigerian arrests and prosecution of some cyber-crime offenders.

Table 4: Cases of Nigerians Arrested and Prosecuted for cyber-crimes

S/N	Cases	Date/Venue	Source
1	The arrest of Joseph Oyediran, an internet fraudster wanted by the Federal Bureau of Investigation, FBI	August 30th, 2019 (Kwara State)	http://www.efccnigeria.org/efcc/news/4771-efcc-arrests-notorious-internet-fraudster-wanted-by-fbi-in-ilorin
2	The arrest of 105 persons and getting 32 convictions which include Ogbonnah Atoukariton and Alpha Chidi Egbeonu an internet fraudster wanted by the Federal Bureau of Investigation, FBI	September 4th (Rivers & Imo states)	https://dailypost.ng/2019/09/04/efcc-arrests-105-cyber-crime-fraudsters-port-harcourt-zone/
3	The arrest of Ajayi Festus, an internet fraudster wanted by the Federal Bureau of Investigation, FBI	August 28th (Ekiti State)	https://www.premiumtimesng.com/news/more-news/349261-efcc-arrests-suspect-who-assisted-nigerian-cyber-crime-syndicate-in-u-s.html
4	Arrest of Ismaila Mustapha and Hamza Koudeih by operatives of EFCC and FBI	November 1, 2019	https://www.pmnewsnigeria.com/2019/11/01/fbi-wanted-cyber-criminals-tracked-down-magu/
5	The arrest of Precious Ibegbulem, Michael Odishi, Ebuka Kenneth, Akabuke Beluolisa, Chibueze Ezeagwu, Nnamdi Maduekwe, Kingsley Orazulike, Linda Chidera and Uche Nwosu by EFCC for internet fraud.	October 18, 2019	https:twitter.com/officialEFCC/status/1185235129213603843

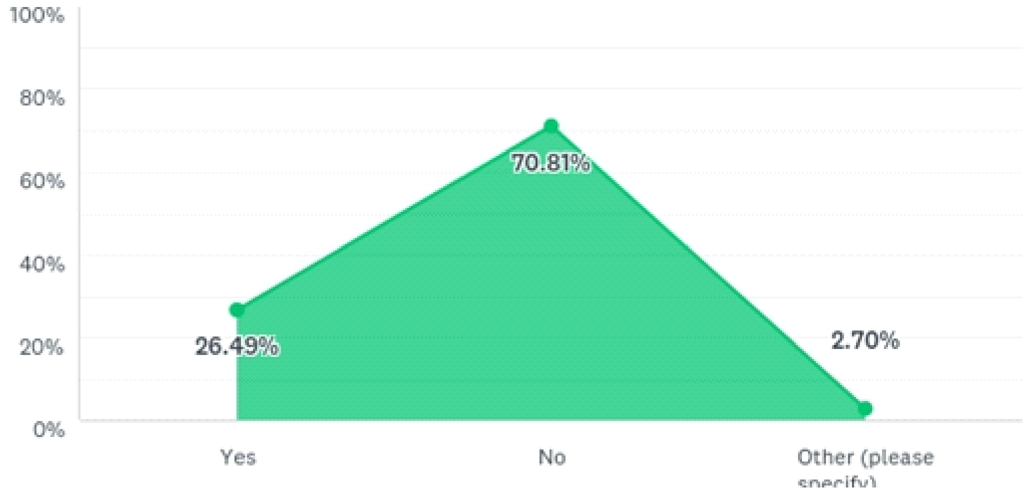
Source: From online newspapers and EFFC official website and Twitter handle

The above is a few of the numerous examples showing the effort of EFCC in fighting cyber-crimes in Nigeria. Although, the cases are quite many it shows the effort of the agencies in tackling cyber-crimes. Despite this concerted effort fighting cyber-crimes in Nigeria, it is still rampant as shown above. More needs to be done because of its far-reaching implications and consequence on Nigeria's image and business. The current effort is like a drop in a million cyber-crimes that are undetected in Nigeria.

Cyber-security and Information Dissemination in Nigeria

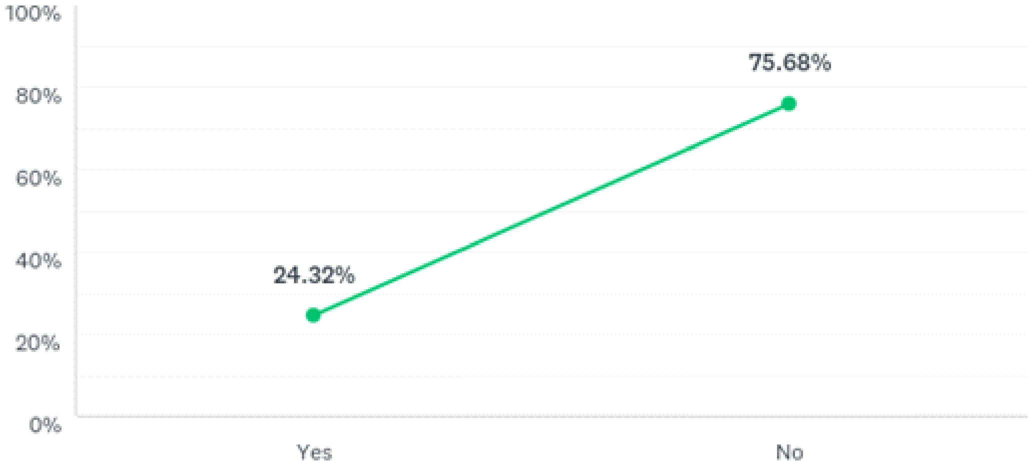
Information and awareness about cybersecurity are quite central to preventing cyber-crimes in Nigeria. The level of cyber-security awareness in Nigeria is low. Many individuals and organisations have rudimentary knowledge about cyber-security and measures to improve them. Around the globe, especially in developed countries, companies are spending millions of dollars to prevent cyber-crimes. Governments are spending huge amount of money to sensitize their citizenry on the threats of cyber-crimes. The quality and quantity of information in Nigeria on cybersecurity are low. Many individuals and organisations take the threat cyber-security pose for granted. The figure below speaks volume of cyber-security in Nigeria. Data gotten from the respondents shows the level of awareness.

Figure 5: Are you aware of Nigeria's Cyber Security Policy?



From Figure 5 above, 70% of the respondent agreed that they do not know cyber-security policies of Nigeria. This shows that many Nigerians are not in the know about cyber-security in the country. It reveals the nature and character of literacy about cybersecurity in Nigeria. The low level of information has led to the growth of cyber fraud in Nigeria. This poor knowledge has not helped the government or security agencies in the fight against cybercrimes. The next figure clearly shows that many Nigerians lack requisite information about methods or tactics to prevent cyber threats.

Figure 6: Have you received any formal training on internet safety measures?



Information or awareness on methods to prevent cyber-crime is quite low in Nigeria. The above figure shows that over 70. % Respondents lack training on the prevention of cybercrimes. The information level on how not to fall victim to internet fraud is very shallow and not robust. Only about 24% of the respondents agreed that they know how to prevent cybercrimes in Nigeria. This shows that more needs to be done by the cyber-security agencies in Nigeria to create more awareness about how to prevent cybercrimes in Nigeria. In all, the above analyses have shown that Nigerian cyber-security architecture needs to do more to prevent cyber-crimes in Nigeria

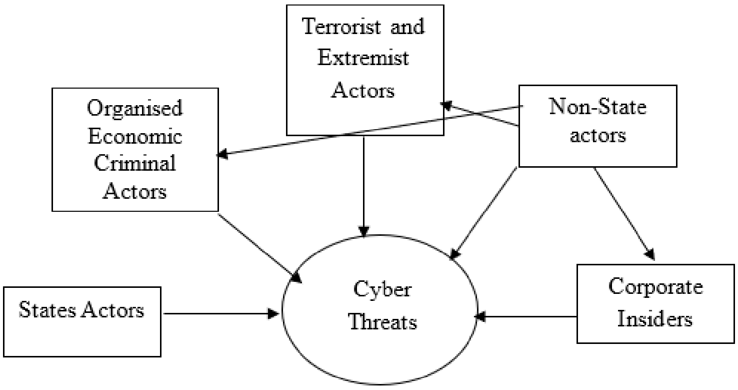
Conclusion

The state's attempts to enhance cybersecurity represents an acknowledgement of the need to widen its conceptualization of security to include societal or sectoral security as advocated by the Copenhagen School' securitization theory. This is because, even though cyber threats affect both the state and the people, the citizens are most vulnerable to cyber threats in Nigeria. Consequently, responses to the management of cybersecurity by the state are predicated upon societal security.

Although the Copenhagen School did not set out to discuss cybersecurity, their concept of human security remains an umbrella term under which to discuss cyber-security. Cybersecurity constitutes an integral aspect of societal security and could as well assume one of the sectoral domains for which security discourse could apply. It should be admitted that cyber threats were yet to occupy the central stage of global socio-political discussion at the time Barry Buzan and his associates began to initiate discussion on reconceptualising security and proposed the widening of the concept to accommodate non-military issues (Buzan et al. 1998; Waever et al. 1993).

Notwithstanding, their seminal contribution is wide enough for a continuous application to non-military issues of society. What is then needed is a novel application of the theory to emerging security threats that are not purely of military nature. Consequently, this study suggests a model of securitization that is considered most appropriate for multi-track responses to cyber threats in Nigeria. It proposes a five-pyramid model of the securitization of cyberspace. The Pyramid Model of Cyber Security (PMSC) proposed in this study begins with the identification and classification of the sources of cyber threats as contained in Figure 7 below.

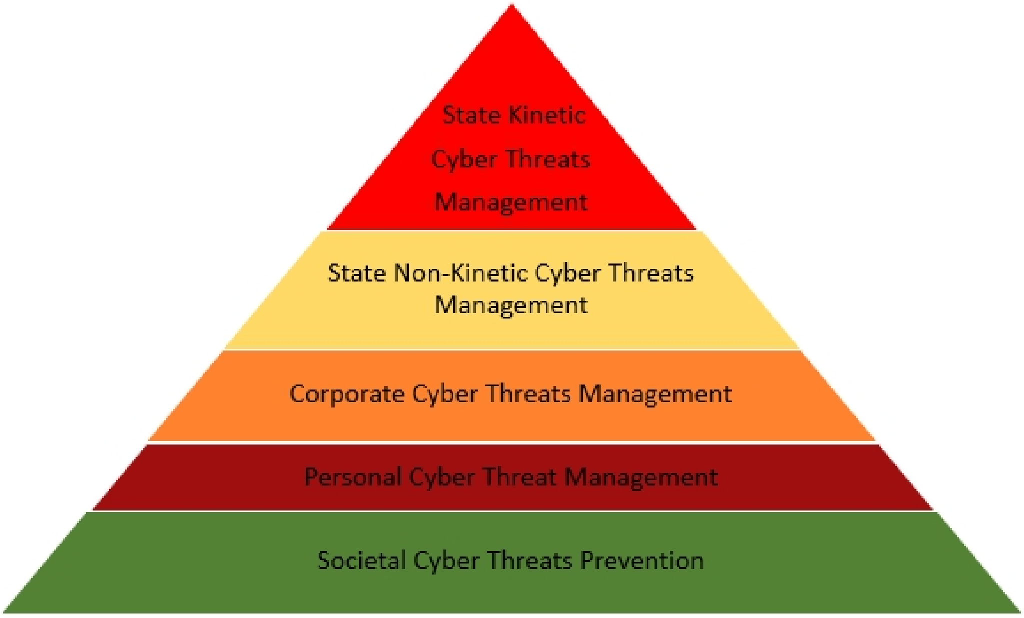
Figure 7: Sources of Cyber Threats


Terrorist and Extremist Actors
Organised Economic Criminal Actors
Non-State actors
Cyber Threats
States Actors
Corporate Insiders

Source: Author (2020)

Identifying the sources of cyber threats is only a first but important step in articulating appropriate responses. Consequently, the PMSC, as seen in Figure 8 articulates a collective security type of responses.

Figure 8: Pyramid Model of Cyber Security



State Kinetic Cyber Threats Management
State Non-Kinetic Cyber Threats Management
Corporate Cyber Threats Management
Personal Cyber Threat Management
Societal Cyber Threats Prevention

Source: Author (2020)

At the base of the PMCS is societal cyber threats prevention. All stakeholders-individuals, corporate organisations, government agencies and state institutions are required to advance preventive measures against the violations of their cyberspace. Preventive measures would include policies that mitigate poverty and diseases within the larger society. Most economic cyber criminals are first attracted to cybercrimes due to poverty and then remain in the act as a result of greed. As the first step, PMCS assumes that once the basic needs of individual members of the society are guaranteed cyber threats will be effectively mitigated.

The second stage in PMCS advocates for the need for individual actors in cyberspace to take charge of the management of their cybersecurity, especially against intruders. The unique nature of cyberspace makes an individual's active participation in the security of the space inevitable. Most victims of petty cybercrimes are generally, tricked into compromising their security. Secured personal cyberspace contributes to the general security of any nation's cyberspace.

Corporate organisations are central to the success of the management of cyberspace. Financial institutions are particularly very useful in the management of cybercrimes at the corporate levels. Most cyber threats against corporate bodies have an economic undertone and banks have become targets of the organised cyber-criminal and other non-state actors. In addition, corporate organisations, especially public institutions would also need to evolve cybersecurity culture, where basic cyber threats preventive and management techniques become part of employee orientation.

The failure of the first three stages of the PMCS will then require the state to activate non-kinetic responses. These would include building cyber resilience infrastructure, regulatory policies that manage national and sub-national data in ways that mitigate or prevent cybercrimes. National non-kinetic responses would also include a robust judicial system, platforms for international collaborations against cyber-criminal elements, technical certification of agencies and organisations in the ICT sector.

The last stage in the PMCS is the use of force against cyber enemies. The state must then be ready and willing to protect this element of human security in securitization the cyberspace against foreign state actors and terror organisation that infiltrate the cyberspace for subversion. While attribution remains a concern in cyber conflict or warfare, the identification of a cyber-aggressor should be adequately responded to even if it has to involve military response. It is, therefore, within this framework that we consider functional multi-track responses to cybersecurity management in Nigeria. This multitrack approach to cybersecurity management agrees with the findings of other scholars such as Sawanah (2020) and Sawaneh, Kamara, and Kamara (2021) equally proposed a multi-stakeholder approach to the management of cybersecurity in Sierra Leone.

References

Băncilă, A. M. (2018). Cyberspace-the new dimension of human interaction. *Scientific Bulletin*, *23*(1), 5-10

Business Journal (2019). *Nigeria Ranks 3rd in Mobile Malware Attacks in 2018.* Retrieved from https://www.businessjournalng.com/nigeria-ranks-3rd-in-mobile-malware-attacks-in-2018/.

Buzan, B., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Chawki, M., (2010). Nigeria tackles advance free fraud, *Journal of Information, Law &amp; Technology* (JILT), & LT; http://go.warwick.ac.uk/jilt/2009_1/chawki&gt

Federal Bureau of Investigation (2019). *US arrests celebrated Nigerian entrepreneurs for fraud*. Retrieved from https://www.cfr.org/blog/us-arrests-celebrated-nigerian-entrepreneur- .

Gartner (2017). *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent from 2016*. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016\\

Institute for Security Studies (2020). *Cybercrime in Nigeria demands public-private action*. Retrieved from https://issafrica.org/iss-today/cybercrime-in-nigeria-demands-publicprivateaction#:~:text=In%202018%2C%20commercial%20banks%20in,537%25%20increase%20on%20the%20N2.&text=Over%2017%20600%20bank%20customers,55%25%20from%20the%20previous%20year

International Telecommunication Union (2018). *Global Cybersecurity Index 2018*. Retrieved from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

Internet World Stats (2020). *World internet usage and population statistics*. Retrieved from: internetworldstats.com/stats.htm

Jack, J.T., & Ene, R. W. (2016). Cybercrime and the challenges of socio-economic in Nigeria. *JORIND* 14 (2). Retrieved from www.transcampus.org/journal; www.ajol.info/journals/jorind

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa, *Journal of Global Information Technology Management*, 22 (2), 77-81

McGuire, M. & Samantha, D. (2013). *Cyber Crime: A Review of Evidence, Research Report 75*. London: Home Office of the UK

Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology*, *7*(2), 61-73.

Norton (2016). *Cyber Safety Insights Report Global Results*. Retrieved from https://now.symassets.com/content/dam/norton/campaign/NortonReport/2019/2018_Norton_LifeLock_Cyber_Safety_Insights_Report_US_Media_Deck.pdf

Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, *6*(3), 116.

Osho O., Falaye, A. A., & Shafi'I, M. A. (2013). Combating Terrorism with Cybersecurity: The Nigerian Perspective." *World Journal of Computer Application and Technology* 1.4 (2013) 103 - 109.

Osho, O., & Onoja, A. D. (2015). National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis. *International Journal of Cyber Criminology*, *9* (1).

Robinson, M., Jones, K., Janicke, H., & Maglaras, L. (2018). An introduction to cyber peacekeeping. *Journal of Network and Computer Applications*, *114*, 70-87

Robinson, M., Jones, K., Janicke, H., & Maglaras, L. (2018). *Developing cyber peacekeeping: observation, monitoring and reporting*. Retrieved from https://arxiv.org/pdf/1806.02608.pdf.

Saulawa, M. A. A., & Abubakar, M. K. (2014). Cybercrime in Nigeria: An overview of cybercrime act 2013. *JL Policy & Globalization*, *32*, 23.

Sawaneh, I. A. (2018) Examining the Effects and Challenges of Cybercrime and Cyber Security within the Cyberspace of Sierra Leone, *International Journal of Intelligent Information Systems*. 7, (3), 23-27.

Sawaneh, I. A. (2020). Cybercrimes: Threats, Challenges, Awareness, and Solutions in Sierra Leone. *Asian Journal of Interdisciplinary Research, 3*(1), 185-195.

Sawaneh, I. A., Kamara, F. K., & Kamara, A. (2021). Cybersecurity: A Key Challenge to the Information Age in Sierra Leone. *Asian Journal of Interdisciplinary Research, 4*(1), 35-46.

Udegbunam, K.C., Akale,C. & Eshilama, B.E. (2021) Cyber warfare and national security in Nigeria, *International Journal of Mechanical and Production Engineering Research and Development*, 11, (3), 561–572