Cybersecurity and Cybercrime in Nigeria: The Implications on National Security and Digital Economy

Babayo Sule (Department of Political Science, Federal University of Kashere Gombe, Gombe State Nigeria); Bakri Mat (School of International Studies, Universiti Utara Malaysia); Usman Sambo (Department of Public Administration, Yobe State University, Damaturu, Yobe State Nigeria); Mohammed Kwarah Tal (Department of Political Science, Federal University of Kashere Gombe, Gombe State Nigeria); and Muhammad Aminu Yahaya (Department of Public Administration, Gombe State University Gombe State Nigeria).

*Corresponding author: babayosule@gmail.com

Abstract

This study examines the implications of cybercrime and weak cybersecurity defense for Nigeria’s national security and digital economy from the perspective of nontraditional discourse within international security debates. The research adopted a qualitative approach to data collection and analysis, with both primary and secondary source data employed. The primary data involved in-depth interviews with selected informants from the relevant agencies in Nigeria and the available governmental policy documents on cybersecurity and cybercrime, including conversations with security personnel, academics, senior officials from security research institutes, members of private institutions and government agencies in communication sectors. The secondary data consist of books, journals, and internet sources. Our analysis reveals that cybercrime is flourishing in Nigeria undetected, affecting its critical national infrastructure, causing prolonged terrorism affecting national security and the safety of national environment due to weak cybersecurity capability. The article recommends that Nigeria adopt measures toward strengthening its cyberspace and digital environment to prevent crimes and promote national security and the digital economy.

Keywords: Cybersecurity, cybercrime, digital economy, national security, Nigeria, security.

Introduction

The shift in the new paradigm of security discourse that emerged during the era of Cold War and beyond stresses the need to pay attention to nontraditional or nonmilitary threats to domestic and international security (Buzan & Hansen 2009). Indeed, the emergence of widespread security challenges such as marine pirates, flood, drought, diseases, terrorism, environmental hazards, and cybercrimes necessitates the rethinking of the foundation of contemporary global security (Buzan 1983, 4). Cybersecurity in particular poses an unrelenting challenge, threatening the existence of mankind and infrastructures across nation-states. Countries are making serious efforts in protecting their cyberspace from cyberattacks and cybercrimes in the face of threats and vulnerabilities that could cause billions of dollars' worth of loss in properties, cash theft, and the collapse of critical national infrastructures (Fischer 2009). Cybercrime is on the rise globally (Buchanan 2016), affecting individuals, companies, organizations, and governments with damages worth billions of dollars (Antonucci 2017).

Within this context, Nigeria is a developing country battling threats to national security on numerous fronts, both traditional military threats and nontraditional challenges such as hunger, diseases, erosion, sea piracy, drought, flood, terrorism, and the explosion of cybercrime both within and outside its borders. Recognition of this latter threat led to the adoption of a policy document on cybersecurity by the Nigerian government in 2015, a comprehensive policy statement detailing the provisions and efforts of the government aimed at achieving a safer digital environment. Many scholars (Schjolberg & Ghernaouti-Helie 2009; Reveron & Mahoney-Norris 2011; Schjolberg & Ghernaouti-Helie 2011; Singer & Friedman 2014; Mazurczyk, Drobniak, & Moore 2016; Maurer 2018) have pointed out that internet and cyberspace are global and pose multiple vulnerabilities to all nation states, and in fact, studies on Nigeria (Frank & Odunayo 2013; Olayemi 2014; Omodunbi, Odiase, Olaniyan, & Esan 2016; Ajiji 2017; Chukwuma & Mogom

2018; and Mohammed, Mohammed, & Solanke 2019), though scanty on the subject matter, suggest that Nigeria is as vulnerable as other countries in the world to these threats.

The Nigerian case, however, is particularly important in terms of the study of cybersecurity and cybercrime due to its unique set of circumstances. The country is the most populous state in Africa, and by extension, the biggest Black nation on earth. It is the tenth-largest oil producing state and the seventh most populous country in the world. The explosion of internet access in Nigeria should be of prime concern for both policymakers and key players in the world of cybersecurity, as vulnerability in the Nigerian context is always imminent. Yet, comprehensive analysis of Nigerian cybersecurity issues is woefully inadequate, a gap this article seeks to address. In addition to providing an overview of the situation we offer policy suggestions for the Nigerian government on how to improve on the existing cybersecurity infrastructure in the country.

Literature Review

In this section, we discuss some of the empirical and theoretical issues related to the subject matter of study. These include (1) the emergence of cybersecurity as a central global concern; (2) the evolution and character of the global digital economy; (3) the emergence and patterns of cybercrime globally and in Nigeria; (4) policies and regulations related to cybersecurity; (5) Nigerian national security; and (6) Nigerian policy response to cybersecurity concerns and cybercrime.

Cybersecurity in the Global Context

In the contemporary era, the rapid expansion of internet communication technologies and digital activities, particularly the proliferation of cellular phones, has created a new security concern, as large quantities of stored data have become the target of hackers and criminals (Rayes & Salam 2019). Further, financial transactions carried out in the internet arena serve as a clear avenue of vulnerability. With over five billion people in the world possessing mobile phones and over four billion having access to the internet, cybersecurity has become an inevitable and pressing concern (Global Web Index 2019). As cyberattacks by nation-states among themselves and by individual criminals against both states and public users have proliferated, a national security paradigm shift has emerged in intellectual discourses (Reveron et al. 2011). In the specific case of Nigeria, twenty-first-century statistics on mobile owners, internet users, and the digital economy suggest that cybersecurity must be taken as a serious concern by both government and private individuals.

Digital Economy

The digital economy and indeed, digital activities such as e-commerce, e-governance, and e-learning, have been undergoing transformation for several decades. Countries have been moving toward digital space for ease of life since the end of World War II, a phenomenon that dates to the invention of the first computer (Severo 2019, 165). With the emergence of internet services, digital activities began to proliferate in the 1980s (Noam, 2019). The contemporary explosion in internet systems across the globe and the creation of communication gadgets such as mobile phones, laptops, iPad, tablets, and other gadgets that use internet services has effectively succeeded in digitalizing the world (Schwanholz & Graham, 2018).

In terms of commerce, by the twenty-first century, many businesses had adopted technology aimed at innovation and improvement of customer services and operations, often with positive results in terms of profitability and ease of operations. The advantages of conducting business online are such that in 2018 more than 42 percent of business globally were conducted in this manner (retrieved from https://www.slideshare.net/sap/99-facts-on-the-future-of-business-in-the-digital-economy-2018). At the same time, enterprises that have done so face the risk of unauthorized use and malicious attacks, including theft, the destruction of intellectual property, abuse by insiders, and illegal use of information, which is tantamount to the loss of data reliability and confidentiality and affects the levels of trust between enterprises and their users/customers (Shalhoub & Al Qasimi, 2010).

In an environment where the digital economy is characterized by the physical separation of the buyer from the seller, the separation of the buyer from the product, and the risk of cybercrime, enterprises must find ways of initiating and developing cyber relationships with customers in sustainable ways, of which the best is establishing a trusted digital space. (Shalhoub & Al Qasimi, 2010). The importance this point is underscored when we consider that most countries in the world are currently going digital in virtually all aspects of national importance, such as e-governance, e-commerce, e-voting, e-transaction, e-learning, and other vital aspects of human endeavor in the society. Digital trust and security in this case take on paramount importance and demand the attention of policymakers.

Emergence and Patterns of Cybercrime

Cybercrime emerged historically in the 1970s and 1980s during the Cold War era. During that period, most patterns of cybercrimes revolved around nation-states engaged in the ideological battle and involved attacking the computers and data of rival countries. Important data related to nuclear proliferation, intelligence movements, and foreign policy were the subject of hacking by professionals employed by the relevant governments. At the same time, individual criminals were also actively hacking data, targeting critical national infrastructures and financial organizations for the purposes of stealing of money and sabotage (Kshetri 2019; Mordi 2019). However, in terms of its pervasiveness, cybercrime became far more extensive, dynamic, and pervasive after the collapse of the USSR.

Cybercrime is believed to have generated an amount of money worth $1.5 trillion in 2018 and $2 trillion in 2019 across the globe through major hacks and thefts from websites and organizations. The annual total amount (that we know of) realized from cybercrimes consists of

$860 billion from illegal online markets, $500 billion from trade secrets and IP thefts, $160 billion from data trading, $1.6 billion from crimeware; and $1 billion from ransomware. In the United States, cyber frauds led to losses of $25 billion in 2010 alone; in Britain and Australia, losses in 2015 amounted to 3.6 billion British pounds and AU$94 million. These crimes have largely involved multinational corporations and governmental information, with major examples of data breaches in 2018 including Yahoo ($3 billion), Under Armour ($150 million), eBay ($145 million), Equifax ($110 million), Facebook ($87 million), JP Morgan Chase ($76 million), Paystation ($77 million), Uber ($57.6 million), and Home Depot ($56 million) (Re-Hashed 2019).

Turning to Nigeria now, similar to other developing countries, the level of development in internet and cyberspace in the 1970s and 1980s in that country was minimal. Even though it was an appendage of capitalist states during the Cold War, cybercrimes in Nigeria during this time were practically nonexistent. Beginning with the 1990s, however, Nigeria joined the retinue of states facing nonmilitary security threats, with cybercrime front and central. For instance, if Africa as a whole lost $3.5 billion in 2017 to cybercrimes, the Nigerian portion of this sum was $645 million, by far the largest (Kshetri 2019). A year later, it was reported that Nigeria lost $800 million (N288 billion) collectively to cyberattacks in 2018 (Azeez 2019). More broadly, a 2019 report disclosed that Nigeria has lost on average N127 billion ($328,842,878 million) annually to cybercrimes in recent years (Ohwovoriole 2019). Furthermore, Nigeria has the reputation of being the global headquarters of cybercrimes, due to frequent daily incidences linked to the country (even though Statista data in 2017 did not even mention Nigeria among the top twenty countries in terms of the highest incidence of cybercrime) (Mordi 2019). Finally, in addition to these glaring threats posed by cybercriminals to the Nigerian economy, the Nigerian Communication Commission (NCC) reported in 2018 that there were about 9 million unregistered lines in the country that were used by mobile owners; some of these were clearly being used for criminal activities such as terrorism, rural banditry, communal violence, kidnapping and robbery, posing a serious threat to national security.

Policies and Regulations on Cybersecurity

The need for policies on cybersecurity is anchored in the recognition that there has been a shift in global governance toward e-governance and the security implications arising therefrom. The 2009 cyberattacks on South Korea and United States present a good case for concern in this regard (Andreason 2012, 77). According to Pelton and Singh (2015), cybersecurity laws should target four major areas. The first is personal and family protection, which consists of protecting stocks, bonds, bank accounts and credit cards, Medicare accounts, desktop computers and Wi-Fi, personal cell phones, and family records. The second aspect involves cybersecurity policies for smart phones and free Wi-Fi that operates through mobile phone security and access. The third aspect is protecting vital infrastructure through the application of satellites with cybersecurity implications. Finally, the fourth is strict government regulation and monitoring of cyber activities. The reality, however, is that the development of such policies has been haphazard at best.

In an attempt to minimize the rate and severity of cybercrimes, various international organizations have undertaken the responsibility of pushing toward cyber law development in both the developed and developing countries. A leader in this respect, the International Telecommunications Union (ITU) launched the Global Security Agenda in 2007 and formed a High-Level Expert Group to investigate the issues and develop proposals for long term strategies (Shalhoub & Al Qasimi 2010, 18). The ITU in particular promulgates laws under its auspices that have some applicability to information warfare attacks that use the electromagnetic spectrum or international telecommunications network (Greenberg, Goodman, & Hoo 1998, 7).

On the state level, governments have adopted antihacking laws to help promote cybersecurity and attempted to approach the issue within the framework of the internationally recognized right of nation-states' rights to defend themselves when attacked, in accordance with article 51 of the UN Charter (Guiora 2017, 63). The Convention on Cybercrime, initiated by some European countries, is the only international agreement in existence at the global level in the area of cybercrime. It is also open for membership to countries outside of Europe, being signed for example by the United States, Canada, Japan, and Australia. The convention comprises three key areas: substantive law, procedural requirements, and international cooperation. However, some critics argue that these laws are outdated and have failed to help effectively protect either private or government computers (Kosseff 2017). Further, as observed by Maurushat (2013), the challenges of laws related to cybercrime are many, including but not limited to the issues of freedom of expression/freedom of speech, copyright, tort of negligence, defamation, illegal telecommunications interception (surveillance), privacy law, data protection, and data breach notification.

National Security

The traditional thinking on national security was predicated on the assumption that state actors are the major players in national and international politics (Buzan 1983, 2). A new conceptual paradigm depicts that national security and indeed, international security, is more complex and dynamic in the post–Cold War era because of the emergence of nonstate actors as powerful players in national and transnational politics (Buzan & Hansen, 2009, 9). Indeed, the failure of the balance of power that had reigned after World War II highlighted the importance of collective security in the international system (Johari 1997, 215). To this end, a number of solutions have been proffered, of which perhaps the most prominent is the deterrence theory as advanced by Realist theorists such as Henry Kissinger (Taylor 2012).

Generally speaking, the national security policy of any state must identify threats domestically and contain them accordingly before expansion toward the global level. Every state may be involved in permanent warfare; control over subversion must be through domination and natural leadership, which is attainable through armed forces (Chomsky & Herman 1979). At the same time, in the present-day national security must address more than just military threats, to include climate conditions, social settings, political structure, the economic basis of the country, among other aspects, with cybersecurity prominent among them. With this context in mind, we now turn briefly to a discussion of national security issues in contemporary Nigeria.

Nigerian National Security

Nigeria's national security policy emphasizes domestic protection, African unity, peace, and the promotion of global peace and security through cooperation, noninterference, and respect for the dignity and value of mankind. Since political independence in 1960, Nigeria has adopted many measures to ensure that the country would protect itself adequately while extending its influence at the African level and globally (Yakubu 2012, 12). Of these goals, the fundamental objective is the protection of the lives and properties of all the citizens and other inhabitants of the country. This is meant to be achieved through building social cohesion, economic prosperity, and mutual coexistence between different groups. Ostensibly, the Nigerian defense strategy is anchored in the understanding the centrality of the recognition of the dignity of mankind, personal well-being, and prosperity before other issues (Alkali 2010, 10). However, the failure of policymakers to in fact pay adequate attention these values and ideals created a huge security gap, which manifested in 1967 through the civil war and later in recent years through terrorism, communal clashes, political violence, rural banditry, kidnapping, robbery, and cybercrimes.

Currently, Nigeria faces many security challenges, both internally and externally. Within the country, the volatile political environment and fragile social settings emanating from multireligious, multiethnic, and regional politics have contributed to security dilemmas, exacerbated by a large contiguous geography, porous borders, and economic problems. The Anglophone and Francophone dichotomy is another security concern, in which Nigeria is surrounded by four major West African countries with a French colonial past, creating a wide gap in terms of communication, external allegiance, and cooperation (Yakubu 2012, 14). More recently, Nigeria has come to face a new security threat, namely, terrorism, with the emergence of the Boko Haram, which shields itself under the umbrella of religion to commit heinous crimes against mankind in the northern part of the country, particularly the northeastern enclave. Within this context, Sule et al. (2019) have suggested that the major focus of the Nigerian security apparatus should pivot toward a nontraditional approach based in cybersecurity and intelligence gathering to address nontraditional/nonmilitary threats.

Nigerian Policy Response to Cybersecurity and Cybercrime

In Nigeria, the Cybercrimes Prohibition Act of 2015 is the major policy instrument meant to boost cybersecurity and prevent cybercrimes in the country. The policy document reiterates unequivocally that the major aim of the act is the prevention of damage to critical national infrastructure (part II, sec. 3 and 4). The act describes those offenses that are considered to be cybercrimes and punishable by law (part III, sec. 5 to 36), including:

- offenses against critical national information infrastructure;
- unlawful access to a computer;
- illegal registration of a cybercafé;
- system interference;
- interception of electronic messages, email, or electronic money transfers;
- tampering with critical infrastructures;

- willful misdirection of electronic messages;
- unlawful interceptions;
- computer related forgery or fraud;
- theft of electronic devices;
- unauthorized modification of computer systems;
- network data and system interference;
- fraudulent electronic signature;
- cyber terrorism;
- exceptions to financial institutions posting and authorized options;
- fraudulent issuance of e-instructions;
- fraudulent reporting of cyber threats;
- identity theft and impersonation;
- child pornography and related offenses;
- cyberstalking or cybersquatting;
- racist and xenophobic offenses;
- conspiracy;
- importation and fabrication of e-tools;
- breach of confidence by service providers;
- manipulation of ATM/POS terminals;
- spreading a computer virus;
- electronic card–related fraud and use of a fraudulent device or attached emails and websites (Cybercrime Act, 2015).

The punishments stipulated for the above identified cybercrimes offenses vary but are related in terms of their severity. Some are punishable with ten-year imprisonment without an option of a fine while some risk up to fifteen years without an option for a fine. Others are punishable with a three-year imprisonment or an option of a fine amounting to seven million Niara.

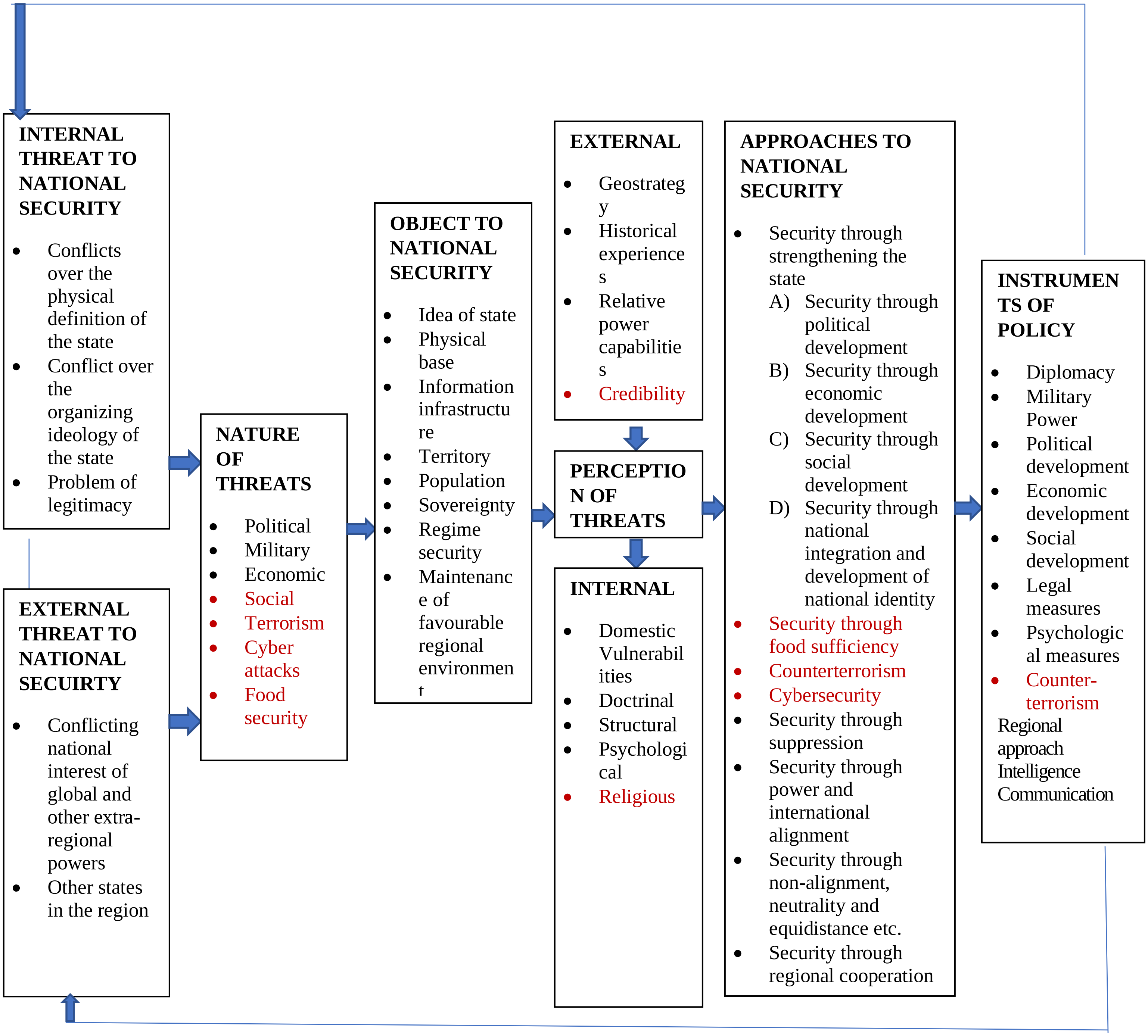
The Case Study and Methodology

As of 2018, the Global Web Index reported Nigeria's population to be 203.6 million, with 169.2 million (83 percent) having mobile phone connections. 89.49 million (42 percent) are internet users and 27 million (13 percent) are active social media users. The digital growth indicators in 2020 from that of 2019 indicate an increase of 5.1 million (2.6 percent) million in Nigerian population. These figures indicate an important threshold in the study of internet and digital communication in Nigeria.

Theoretical Framework: National Security of Developing Countries Model by Alagappa (1987)

This work adopts and expands the on the "National Security of Developing States" model postulated by Muthiah Alagappa (1987), presented and discussed below. We did so for three reasons. The first has to do with the chain of values and clear illustrations that are depicted in the diagram for easy grasp of the concepts involved, namely, national security and possible vulnerabilities and threats. Secondly, previous studies on our case have used other theories, such as political realism, collective security, foreign policy analysis, and other related frameworks, but none of them refer to this framework, clearly demonstrating the innovative nature, contribution, and new ideas proposed by this study. Thirdly, the theory as it stands leaves room for future theory building. Originally developed in 1987, the theory identified some internal and external threats to national security of developing countries at a time when cybersecurity and cybercrime in developing countries were practically nonexistent. But its postulations left the door open to explore threats in the political, social, economic, and environmental areas, making it easy for researchers to lean on the original postulations and build on the theory for further development of knowledge in the field of social sciences.

Figure 1: The National Security of Developing States: A Framework of Analysis


INTERNAL THREAT TO NATIONAL SECURITY
Conflicts over the physical definition of the state
Conflict over the organizing ideology of the state
Problem of legitimacy
EXTERNAL THREAT TO NATIONAL SECURIRTY
Conflicting national interest of global and other extra-regional powers
Other states in the region
NATURE OF THREATS
Political
Military
Economic
Social
Terrorism
Cyber attacks
Food security
OBJECT TO NATIONAL SECURITY
Idea of state
Physical base
Information infrastructure
Territory
Population
Sovereignty
Regime security
Maintenance of favourable regional environment
EXTERNAL
Geostrategy
Historical experiences
Relative power capabilities
Credibility
PERCEPTION OF THREATS
INTERNAL
Domestic Vulnerabilities
Doctrinal
Structural
Psychological
Religious
APPROACHES TO NATIONAL SECURITY
Security through strengthening the state
A) Security through political development
B) Security through economic development
C) Security through social development
D) Security through national integration and development of national identity
Security through food sufficiency
Counterterrorism
Cybersecurity
Security through suppression
Security through power and international alignment
Security through non-alignment, neutrality and equidistance etc.
Security through regional cooperation
INSTRUMENTS OF POLICY
Diplomacy
Military Power
Political development
Economic development
Social development
Legal measures
Psychological measures
Counter-terrorism
Regional approach
Intelligence
Communication

Source: Muthiah Alagappa (1987). Expanded by the researchers.

The above model indicates that there are, esentially, two major threats to national security: internal and external threats, with both being possibly either traditional or nontraditional. In the internal case, there may be social incoherence and other vulnerabilitites that might lead to armed groups—which is a traditional threat—while at the external level there might be territorial and national interest issues that might set one country at conventional military conflict with another. From the nontraditional perspective, issues such as the economy, geography, social settings, or sea and land rights can be potential conflicts that might lead to insecurity internally and externally for developing states like Nigeria. For example, case of Boko Haram here falls within both the traditional and nontraditional threats and internal and external security threats that Nigeria is facing. The nature of threats can be economic, military, political, or, as we propose in this research, related to terrorism, food insecurity, or cyber attacks. Thus, as identified by Alagappa (1987), any serious developing country that seeks absolute national security must pay attention to both internal and external security and also must give consideration utmostly to both the trational and nontraditional military threats.

The framework advanced by Alagappa (1987) is suitable for this study because it has the leverage of providing an all-round explanation of national security of countries like Nigeria, that is, accounting for both traditional and nontraditional threats. Other theoretical frameworks discussed in the above section can explain either the political angle or the economic perspective of cybersecurity and cybercrime. However, the theory we lean upon is all-encompassing in terms of both theoretical and empirical analysis. For instance, looking at the figures of users of mobile phone and internet in Nigeria and examining the loss of billions of dollars in cybercrime, one can easily use this framework to establish and illustrate that the phenomena are related to national security. The trillions of Naira deposited in Treasury Single Account (TSA) by the government and the hundreds of billions used monthly for the payment of salaries under the Integrated Personnel Payroll Information System (IPPIS) present a node of vulnerability if the Nigerian cybersecurity system is hit. In our work, we rely on empirical evidence related to cyber communication by criminals and terrorists in building the theoretical apparatus. In essence, our empirical findings strongly support the theory's suggestion that nontraditional security threats to countries like Nigeria can be as strong as traditional ones.

Our work is inspired, certainly, by that of others. For instance, Cavelty & Wenger (2019) opined that there is a great deal of effort within the international relations discipline aimed at situating its analytical discourse toward an inclusive focus on cybersecurity as a part of global security concerns. Cavelty et al. (2019) stress that cybersecurity is connected to political security because state actors are dealing with state and nonstate actors on the international scene whenever there are threats and vulnerabilities of attacks from a perceived hostile enemy. Cavelty et al. (2019) presented three key drivers that influence cybersecurity politics and research in the field. They include politics (divided into domestic politics and international politics), science (consisting of academic debates and institutionalization), and technology (involving key events and development and use). One of the areas that this research is interested in is domestic and international politics of Nigeria with regard to cybersecurity, and of particular relevance to us is that Cavelty et al. (2019) found it expedient to expand the rationale behind why research of this nature is undertaken from the theoretical perspective.

There are other studies (Koops 2016; Aniekan & Afolabi 2017; Diogenes & Ozkaya 2018; Kremling & Parker 2018; and Kshetri 2019) similar to that of Cavelty et al. (2019) on the nature and necessity of undertaking cybersecurity research and cybercrime protection from the perspective of politics. These studies suggest strongly that any serious country and indeed other organzations as well as individuals today must have a serious provision and concern for securing their personal belongings, data, and environment against political attacks via cyberwarfare. The Nigerian case is especially pertinent because of the shortage of adequate research on the political implications of cybersecurity in the country from the vantage point of national security. Research of this nature should be of paramount importance not only for policymaking but also for setting the foundation of future research on cybersecurity and politics in the Nigerian contexts and by expansion, in Africa. Finally, we should note an interesting work (World Bank, 2017) that emphasizes more the digital aspect of the question: namely, the World Bank posits that the extent to which consumers and organizations are going digital makes it imperitive for countries to secure their cyberspace.

The theoretical and empirical contribution of our research supports the conclusion that the assumptions and strategies presented by the likes of Alagappa (1987), Cavelty et al. (2019), and Kshetri (2019) for identification of cybersecurity as a nontraditional political security threat that requires counteraction should be analyzed and digested by researchers and policymakers in the area of study. To reiterate, we settled ultimately for Alagappa's model because of its permeability, comprehensiveness, and wider horizon in embracing all the elements and variables discussed in the study, such as national security, cybersecurity, cybercrime, digital economy, policy responses, and collective security in general.

Data Collection and Analysis

Primary source data came from interviews with some selected participants drawn from different categories, as well as from the policy document on cybersecurity adopted by the Nigerian government and other reports from relevant agencies. A total number of thirty interviewees were selected, to be sorted in four categories coded as category A, B, C, and D. In category A, eight military or paramilitary security personnel were selected from different agencies directly dealing with security issues. A senior security officer in Nigerian military was selected based on accessibility and possession of quality relevant data on the subject matter of study; another senior officer from the Nigerian Police Force was chosen based on accessibility and possession of valuable information. Other interviewees in this category included a senior officer from the Department of State Security, a senior officer from the Nigerian Immigration Services, a senior officer from the Nigerian Prison Services, a senior officer from the Nigerian Security and Civil Defense Corps, a senior officer from the Nigerian Custom Services, and a senior officer from the Nigerian Federal Road Safety Corps.

In category B, ten senior officials were chosen from institutes and agencies handling security issues, including two senior officials from the National Institute for Policy and Strategic Studies (NIPSS) Kuru Jos, two senior officials in the National Defense Academy (NDA), two senior officials from the Nigeria Police College Wudil Kano, two senior officials from the Ministry of Defense, and two senior officials from the National War College Abuja. For its part, category C comprised academicians, wherein six professors were selected from three universities based on the proximities of the researchers. Two are professors in political science with specialization in security and strategic studies from a reputable national university, two are professors of computer science with specialization in cybersecurity and digital environment, and the last two are professors of sociology with specialization in criminology from a reputable national university.

In category D, six members of private institutions that deal with cyber activities were selected randomly and interviewed. These comprise a senior bank official in Abuja in one of the commercial banks, two senior officers from the telecommunications companies operating in Nigeria, a senior official in the Nigerian Communication Commission (NCC), a senior official from the Nigerian Technology Development Agency (NITDA), and a senior official from the

Federal Ministry of Communication. All of them were selected and interviewed in Abuja, where their head offices are located.

There were three criteria used to identify the informants to be interviewed for this study. The first was the identification of stakeholders who are closely linked and related to the subject matter of national security, cybersecurity, and cybercrime and digital economy. The researchers were instructed by various agencies and ministries to consult staff or units on cybersecurity in security parastatals and other ministries. They were directed by senior officials there to consult the most informed in the unit on the subject matter of cybersecurity. The selected informants were interviewed based on the condition of anonymity and confidentiality. The second criteria used was the accessibility. For instance, academicians who were consulted were chosen based on accessibility in addition to their possession of in-depth knowledge on the subject matter; the same was true for some government ministries and agencies. The third criteria used was based on Sharan′s postulate (2009) that the minimum number of interviewees for a qualitative research project should be either four or five and that the maximum should be thirty, depending on the availability of the resources and informants with quality information.

While the questions were prepared separately for each category, some general questions were posed to all four categories of interviewees. Semistructured questions were designed to enable for flexibility and free flow of information from the informants. The method used for gathering the data was written questionnaires organized in semistructured sessions, adapted to the different categories of the informants. Some of them were interviewed through phones, some responded through email, and others through WhatsApp.

Finally, as mentioned, the other primary sources of data included the government policy document on cybersecurity enacted in 2015 by the Nigerian government, together with various reports by national and international agencies on cybersecurity in Nigeria. Secondary sources consisted of books, journals, and internet sources relevant to the topic at hand. The data obtained were grouped into themes and analyzed using content analysis in which the previously existing literature was analyzed in relation to the findings of this work and the application of the theoretical framework for conclusion and findings.

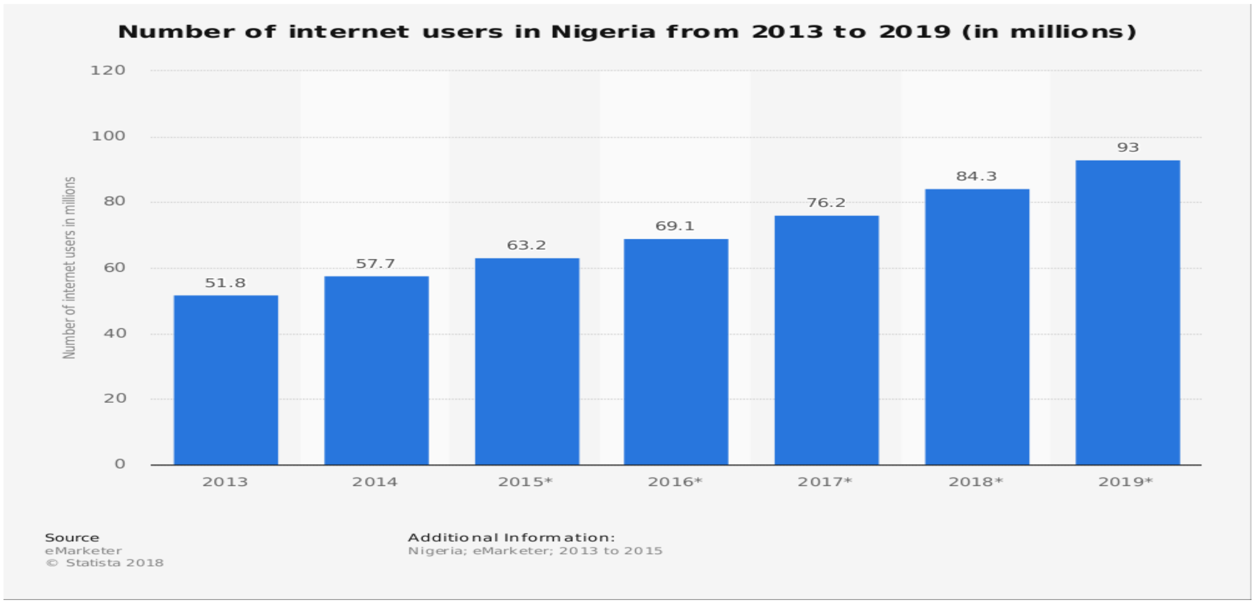
Discussion and Findings

This section discusses the major findings from the fieldwork, contextualizing it within the existing literature and the adopted theoretical framework, which enabled the identification of the knowledge gap and contribution to knowledge. The data are discussed in thematic form under three major themes: perspectives on challenges and prospects of cybersecurity in Nigeria, the effects of cybercrimes on Nigeria's national security, and implications of cybercrime for the digital economy.

Perspectives on Challenges and Prospects of Cybersecurity in Nigeria

We have previously noted the rapidly increasing number of internet and computer users in Nigeria, a population that is vulnerable to cybersecurity breaches and cybercrime. The potential for negative outcomes has been further escalated with the emergence of social media usage in the country, to include emails, Facebook, WhatsApp, Telegram, YouTube, Instagram, and many other technologies. In addition to data presented earlier, we should note that digital growth indicators from 2019 to 2020 show that mobile connections increased by 12 million (+7.7 percent), the number of internet users grew by 2.2 million (2.6 percent), and active social media users increased by 3.4 million (14 percent). These data substantiate the conclusion that Nigeria has been going digital rapidly in recent years: for example, from 2013 to 2019 the number of internet users increased from 51 million to 93 million, as seen in figure 2.

Figure 2: Number of Internet Users in Nigeria from 2013 to 2019



Source: Adopted from Statista 2019.

Another source from the Nigerian Communication Commission (NCC) disclosed the figure of internet users in Nigeria as 111.6 million in December 2018, an increase of more than 10 million over Statista's data. In any event, the increase in the use of social media also contributes to the vulnerability and exposure of the private users and government agencies, organizations, and corporations to cybercrime.

The figures above imply that there is a clear need in Nigeria for allocating a huge sum of money and adopting a strong policy on cybersecurity in order to minimize vulnerability and effectively combat related crimes. Indeed, this was the justification for the adoption of the Cybersecurity Act in 2015. On the other hand, Nigeria faces a serious challenge in the cybersecurity sector because of poor infrastructure, low levels of digital know-how and low-level information transmission. The 2018 Cybersecurity Index concisely pinpointed Nigeria's vulnerabilities in this regard (table 1).

Table 1: Nigeria's Cybersecurity Index 2018

Rank	National Cybersecurity Index	Digital Development Level	Difference
45	44.16	35.86	8.30

Source: Global Cybersecurity Index 2018.

And yet, not all of our sources viewed the prospects of and challenges to cybersecurity in Nigeria in identical ways. We summarize and present their views here in tabular form (table 2).

Table 2: Responses of Informants on the Prospects and Challenges of Cybersecurity in Nigeria

Category	Informants	Prospects	Challenges
A	1	Strong rules and regulations	Lack of enforcement
	2	Improved awareness	Information flow
	3	Existence of cybersecurity laws	Lack of adherence to rules
	4	Global cooperation and interconnectivity	Borderless crimes
	5	Increase users and malware protection	Anonymity aspect
	6	Global awareness forum and policies	Weak digital know-how
	7	Increased protection through policies	Poor management of cybersecurity
	8	Low level of internet users	Vulnerability
B	1	Emergence of sanctions on cybercrime	Borderless nature of internet
	2	Availability of policies on cybersecurity	Vulnerabilities in the cyberspace
	3	Increased information flow	Low level of infrastructure
	4	Emergence of programs on cybersecurity	Limited number of experts
	5	Technical support from advanced countries	Suspicion and lack of digital trust
	6	Bridging the knowledge gap on internet	Low level of information flow
	7	Establishment of cybersecurity laws	Failure of enforcement by authorities
	8	Digital protection through policies	Anonymous and external threats
	9	Training and modern equipment	Low technical support in operation
	10	Points for identifying suspicious activities	Corruption and mismanagement
C	1	Increasing the horizon of security studies	Inadequate professionals and experts
	2	Existence of specific policies and sanctions	Lack of adequate awareness
	3	Global awareness and technical support	Vulnerability and human rights
	4	Increasing conscience of the public	Global nature of cyberspace
	5	Strong policy and performance	Low level of protection
	6	Spying on criminals for detection	Infringement on privacy
D	1	Low level of digital activities	Lack of knowledge on the field
	2	The presence of regulations	Fragile security situation
	3	Training of professionals for cybersecurity	Lack of political will
	4	Management information flow system	Lack of qualified manpower
	5	Digitalization policies by the government	Lack of awareness of the threats

6	Resistance to fraudsters and cybercriminals	Increase number of internet users

Source: Field Survey from interviews conducted between July to December 2018 with the selected informants by the researchers.

In addition to the summary above, there are one or two views that are revealing and should be expressed here. In an interview, one of the informants narrated that “Nigeria is tilting towards cyberspace like other world countries but there is a huge challenge that should awaken the policymakers towards particularly securing the cyberspace through an effective cybersecurity. This is because Nigeria lost N288 billion in 2018 alone to cybercrime which is alarming and a threat to the internet users in the country” (Interview with an informant in category A on October 27, 2018, in Abuja at 11:30 am). From a different perspective, another informant revealed that “the weak cybersecurity space in Nigeria disclosed how vulnerable the country. Nowadays, we are no longer battling with terrorism alone but cyberterrorism because even the terrorists themselves were using the cyberspace through the anonymity doctrine to undertake their heinous crimes” (Interview with an informant in category C on September 18, 2018, at 9 am).

Effects of Cybercrime on National Security in Nigeria

Cybercrime has now become a major security headache across the globe because of its nature, which is cross-border, anonymous, and very difficult to detect or prove. In Nigeria in particular, the cybercrime indices indicate a harmful and vulnerable situation, with the country listing among the ten top countries in the cybercrime index as reported by US Federal Bureau of Investigation. The report revealed that the United States ranks first, United Kingdom second, Nigeria third, followed by Canada, Romania, Italy, Spain, South Africa, Russia, and China. Apart from the above, the interviewed informants revealed different views on the effects of cybercrime on national security in Nigeria. The views are summarized and presented below in a tabular form (table 3).

Table 3: Summary of Informants Views on the Effects of Cybercrimes on National Security

Category	Informants	Responses
A	1	It creates room for terrorism
	2	It escalates insurgency
	3	It creates fear and spread of undetected crimes
	4	It leads to the spread of insecurity in all parts of the country
	5	Resources in billions are lost annually
	6	Kidnappings and other crimes are flourishing undeterred
	7	Vital national information is accessed without authorization
	8	People are not safe in the country, including security personnel
B	1	Critical national infrastructure is at risk
	2	Individuals are affected in their private dealings
	3	Terrorists are utilizing cyberspace for coordination of attacks
	4	Internal and external fraudsters are defrauding Nigerians undetected
	5	Security personnel are finding it difficult to handle insurgency
	6	Counterinsurgency is facing setbacks because of the use of the internet
	7	Criminals are extorting billions of naira through e-fraud
	8	The economy is affected through cybercrimes
	9	The social setting is suffering from crimes undertaken using internet
	10	The emergence of cellphones allows for cybercrimes and insecurity
C	1	Cybercriminals use smartphones and internet for their activities
	2	Terrorism is increased by cyberspace through internet communication
	3	External treats exist trough e-attacks on digital businesses
	4	Hacking of organizational data leads to stealing of billions of naira annually
	5	The national economy is dragged backward because of threats
	6	The digital economy is sluggish due to fear of cybercrimes
D	1	Cybercrimes lead to increased terrorism which affects national security
	2	Online businesses are affected by cybercrimes via mutual suspicion
	3	Vital governmental information is accessed by unauthorized persons
	4	National security planning is at risk of hacking by criminals
	5	Use of private cellphone and emails exposes individuals
	6	Individuals are tacked and targeted through cyberspace

Source: Field survey from interviews conducted between July to December 2018 with the selected informants by the researchers.

In an interview, one informant underscored a crucial point, namely that “critical national infrastructures are at great risk in the country such as payment platform like IPPIS and Treasury Single Account as well as many other segments that are using the internet for delivering important services to the nation. The repercussions are that once Nigeria by either advertent or inadvertent accident found itself under cyberattacks, the damage would be unimaginable" (Interview with an informant in category B on November 11, 2018, at 8:30 pm). Furthermore, another informant disclosed that "the global trend for national security is shifting towards cyberspace and collective security is now moving globally towards securing the cyberspace which is more important. Criminal activities that can threaten national security of a country like Nigeria such as terrorism, cyber fraud, looting of national treasury and lack of national databank for emergencies are possible if the cybersecurity of Nigeria is not given adequate attention that it deserves as other world countries are doing today" (Interview with an informant in category D on December 19, 2018, at 11:00 am). Theoretically, the Alagappa model is useful to strengthen the analysis here because the activities of hackers and terrorists as indicated above show that the insecure cyberspace in Nigeria has greatly exposed the country to criminal activities that affect national security.

Additionally, during fieldwork the researchers themselves noted a daily incidence of an average of two mails per day via their emails, where they are targeted for cybercrimes and fraud. Some of the emails bore European, American, or Arabic names, claiming to come from the United Nations and other reputable international organizations; the content of the email would ask the recipients to assist in the transfer of millions of dollars from various world destinations into Nigeria. The targeted individual would be asked to help by providing his account details for the transaction and in return he would allegedly receive half of the proceeds of the transfer. In other mails, the targeted individual would be congratulated and asked to forward his details as the winner of the World Health Organization's annual charity, or a prize given by the United Nations, UNICEF, or other related agencies. All the informants who were consulted as interviewees for this study also attested to the same experience. Sometimes it is a direct call from some unscrupulous elements claiming that you must send your account number and Bank Verification Number (BVN) for rectification of an account issue. Once sent, you will start receiving alerts that you are withdrawing money, your account hacked, and the money stolen. “In essence, once your email is online and you are a frequent user of internet and emails especially academicians who published articles with their details of addresses and other organizations that place the details of their staff on net, you are vulnerable and exposed to these cybercriminals” (Informants in category B, views expressed during an interview on September 17, 2018, at 9:30 am).

In another view, some of the informants also narrated that cybercrimes are carried out through the use of computers and smartphones, leading to national insecurity. For instance, terrorists in Niger-Delta who steal oil and bomb the oil wells and pipelines communicate through phones and emails; similarly, the Boko Haram terrorists carried out their insurgency using internet communication such as computers, YouTube to release video messages, phones, and other means of modern communication. The lack of a proper mechanism put in place by the government to detect the criminals is causing a serious security breach and a potential threat to national security as is now being witnessed where the entire country is enmeshed in one form of insecurity or the other such as Boko Haram in the northeast, armed bandits and kidnapping in the northwest, a Farmers-Herders conflict in the north central region, militants’ activities in Niger-Delta, kidnappings in the southeast and armed robbery in the southwest.

Implications of Cybercrime on Digital Economy

Globally, there are around three and a half billion internet users and five billion mobile phone users. Ninety-nine percent of the world’s population lives in a place that is covered by a mobile-cellular network and 84 percent of people on the planet live somewhere covered by mobile broadband networks (Graham 2019, 3). The above statistics indicate that the world is fast becoming connected by internet and cyberspace activities, including Nigeria, and this by implication means a commensurate rate of cybercrimes and threats to digital economy. Cybercrime in Nigeria in particular has great implications for the digital economy because Nigeria is an emerging economy well-positioned to survive and prosper via e-commerce due to its population of about 200 million, enormous potential market, and diverse natural resources. The above assertion is supported by the statistics below.

The online purchase of consumer goods in Nigeria in 2020 discloses a significant number of users of digital economy in the country. About 76.6 million Nigerians are shopping online, worth an amount of $3.37 billion; 2.2 percent of the GDP comprises the activities of online consumer. The value of the e-commerce market is recorded at $13 billion, which signifies an increase of 42 percent from 2019 and an average of $401 per consumer. Forty percent of transactions in 2020 were conducted using mobile phones. Of the payment method of e-commerce in Nigeria, the following may be said (as of 2020): 27 percent was credit card, 24 percent cash, 23 percent bank transfer, 9.0 percent e-wallet, and 17 percent other. The number of people who are making digital payment transactions is 105 million, with a total annual value of $21.61 billion, signifying an increase of 21 percent from 2019 with $206 as an average digital payment per digital payment user. The value of the total digital advertising market is $1.17 billion, with $412 million spent on digital search ads, $516 million on social media ads, $89 million spent on digital banner ads, $94 million on digital video ads, and $55 million on digital classified ads (Global Web Index 2020).

A summary of the views of the informants on the implications of cybercrimes on the digital economy in Nigeria is presented below in table 4.

Table 4: Summary of the Views of Informants on the Implications of Cybercrime on Digital Economy in Nigeria.

Category	Informants	Responses
A	1	Low level of digital trust
	2	Affect economic growth and development particularly e-commerce
	3	Prevents utilization of cyberspace for jobs creation
	4	Discourages entrepreneurs from initiating a business model on the internet
	5	Leads to loss of billions of USD
	6	Sabotage the economy
	7	Decline in the service sectors and Value Added Tax (VAT)
	8	Stymied modernization of business activities leading to physical transactions
B	1	Affects governmental revenue generation
	2	Consolidates overdependence on oil only as the major source of revenue
	3	Deprives service sectors from performing
	4	The usual relief of physical task of business is not benefitted from [*sic*.]
	5	Many businesses collapsed
	6	It deprives aspiring entrepreneurs of innovation and initiation
	7	Resources are wasted and lost unnecessarily
	8	Lack of confidence and cynicism about digital activities
	9	Secrecy is violated and compromised
	10	Waste of time, energy, and resources
C	1	Lack of digital trust
	2	e-commerce is crippled
	3	Cyberspace is being mis-utilized for social media only, without any benefit
	4	Energy and time is wasted in physical transactions
	5	Risk and uncertainties increased through physical transaction
	6	Valuable services are lost
D	1	People failed to benefit from digital transaction leading to low technological spread
	2	Mis-utilization of cyberspace for trivial activities instead of productive ventures
	3	Corporations are finding it difficult to operate nowadays
	4	Small scale businesses are not developing in e-commerce
	5	Investment is lost and wasted
	6	Public confidence is affected in e-businesses

Source: Field survey from interviews conducted between July to December 2018 with the selected informants by the researchers.

As before, some informants' major points are relevant to be quoted here. One of them disclosed that "the Nigerians are now enjoying digital economy through e-commerce and digital shopping from the comfort of their homes. But inadequate awareness, exposure, vulnerability, and weak cybersecurity is threatening the revolution in digital economy in the country even with the reality that the country can no longer survive without going digital, the colossal loss to hackers and cyber fraudsters recorded in the country disclosed that the digital economy has a serious challenge" (Interview with an informant in category C on August 6, 2018, at 10: 00 am). Another informant revealed that "corporations in Nigeria are finding it difficult to make transaction easier for its customers due to the alarming rate of cybercrime in the country and even the government itself is slow in transferring towards e-governance and e-transaction due to hackers and a weak cybersecurity in the country" (Interview with an informant in category A on August 17, 2018, at 3: 00 pm).

Conclusion and Recommendations

The study concludes that Nigeria has recognized the importance of cybersecurity owing to its establishment of the Cybersecurity Act 2015, as a direct response to the recent emergence of cybercrimes in the country. The study contributed to the scholarly literature both empirically and theoretically. Empirically, the study revealed statistics regarding mobile and internet users in Nigeria as well as digital online activities in the country. It reported scientific views from informants on the effects of cybercrimes on national security and digital economy in Nigeria. Theoretically, the study succeeded in linking the connection between the various existing propositions on matters of national security and cybersecurity and the emerging empirical evidence from the area of study. The study also has policy implications in terms of initiating some proposals for policymaking in cybersecurity to prevent cybercrimes in Nigeria. The recommendations are listed below:

1. The government and other agencies responsible for ICT regulations should create popular awareness on the need to prevent the exposure of security codes and other vital information online;
2. People should be sensitized to report suspicious transactions to the agencies that are responsible for the handling of cybersecurity policies;

3. Experts should be engaged to train existing staff within the relevant agencies on cybersecurity technicalities for easy identification of threats;
4. Workshops and media advertisements should be regularized quarterly to enlighten the public, organizations, and governmental agencies on the workings of cybercrime and how to adopt measures for protection;
5. Those who are caught in cybercrime activities should be punished severely according to the regulations of Cybersecurity Act 2015 to deter other criminals from future occurrence and
6. A databank for internet users and mobile phones should be created to enable the identification of suspicious calls and transactions in order for criminals to be apprehended immediately upon initiating an attack.

Acknowledgement of Funding

The work for this study was undertaken with research grant assistance from Professor Madya Bakri Bin Mat, an Associate Professor of Security and Strategic Studies in the School of International Studies, College of Law, Government and International Studies, Universiti Utara Malaysia.

References

Ajiji, Y. M. (2017). “Cybersecurity Issues in Nigeria and Challenges.” *International Journal of Advanced Research in Computer Science and Software Engineering* 7(4): 315–321.

Alagappa, M. (1987). *The National Security of Developing States: Lessons from Thailand*. Dover, MA: Auburn House.

Alkali, R. A. (2010). *Issues in Nigerian Foreign Policy and International Relations*. Kaduna, Nigeria: Media Press.

Andreason, K. (2012). *Cybersecurity: Public Sector Threats and Responses*. London: Taylor & Francis.

Aniekan, M. N., & Afolabi, M. B. (2017). “Introduction to Cybersecurity and Cybercrime.” In Aniekan & Afolabi (Eds.) *Intelligence and Security Studies Programme*. Lagos, Nigeria: Spectrum.

Antonucci, D. (2017). *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*. Hoboken, NJ: John Wiley & Sons.

Azeez, O. (2019). “Cybercrime Cost Nigeria N288 bn in 2018.” *Business a.m*. https://www.businessamlive.com/cyber-crime-cost-nigeria-n288bn-in-2018/, accessed March 25, 2020.

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012).

Cybersecurity Policy Guidebook. Hoboken, NJ: John Wiley & Sons.

Beissel, S. (2016). *Cybersecurity Investments: Decision Support under Economic Aspects*. Geneva: Springer.

Buchanan, B. (2016). *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations*. New York: Oxford University Press.

Buzan, B. (1983). *People, State and Fear: An Agenda for International Security Studies in the Post-Cold War Era*. Chapel Hill: University of North Carolina Press.

Buzan, B., & Hansen, L. (2009). *The Evolution of International Security Studies*. New York: Cambridge University Press.

Cavelty, M. D., & Wenger, A. (2019). "Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science." *Contemporary Security Policy* 41(1): 1–28.

Chomsky, N., & Herman, E. S. (1979). *The Washington Connection and Third World Fascism*. Boston: Southend Press.

Chukwuma, O. A. I., & Mogom, I. A. (2018). "The Internet and National Security in Nigeria: A Threat-Import Discourse." *Covenant University Journal of Politics & International Affairs* 6(1): 20–29.

Collier, D. (1993). "The Comparative Method." In Ada, W. F. (Ed.), *Political Science: The State Of the Discipline II*. Washington, DC: American Political Science Association.

Diogenes, I., & Ozkaya, E. (2018). *Cybersecurity Attacks and Defense Strategy*. Birmingham, UK: Packt Publishers.

Federal Government of Nigeria (2015). *Nigerian Cybersecurity Act 2015*. http://lawnigeria.com/LawsoftheFederation/Cyber-Crime-Act,-2015.html. Accessed Mar 25, 2020.

Fischer, E. A. (2009). *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*. New York: Nova Science.

Frank, I., & Odunayo, E. (2013). "Approach to Cybersecurity Issues in Nigeria: Challenges and Solutions." *(IJCRSEE) International Journal of Cognitive Research in Science, Engineering and Education* 1(1): 1–11.

George, A. L., & Bennett, A. (2005). *Case Studies and Theory Development in Social Sciences*. Cambridge, MA: Cambridge University Press.

Gerring, J. (2007). *Case Study Research: Principles and Practices*. Cambridge, MA: Cambridge University Press.

Global Cybersecurity Index (2018). *Global Cybersecurity Index*. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. Accessed March 25, 2020.

Global Cybersecurity Index (2019). *2019 Global Cybersecurity Index*. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. Accessed March 25, 2020.

Global Web Index (2020). *The Digital Trends to Watch in 2020*. https://www.globalwebindex.com/reports/trends-20. Accessed March 25, 2020.

Graham, M. (2019). "Changing Connectivity and Digital Economies at Global Margins." In Graham (Ed.) *Digital Economies at Global Margins*. Cambridge, MA: The MIT Press.

Greenberg, L. T., Goodman, S. E., & Soo Hoo, K. J. (1998). *Information Warfare and International Law*. Washington, DC: National Defense University Press.

Guiora, A. M. (2017). *Cybersecurity, Geopolitics and Law*. London: Routledge.

Heintze, H., & Thielborger, P. (2016). "From Cold War to Cyber War: The Evolution of the International Law of Peace and Armed Conflict over the Last 25 Years—An Introduction." In Heintze & Thielborger (Eds.) *From Cold War to Cyber War the Evolution of the International Law of Peace and Armed Conflict over the Last 25 Years*, 3–9. Geneva: Springer.

Internet Crime Complaint Centre, FBI (2018). *Cybercrime Statistics: Top Ten Countries in the World*. https://www.ic3.gov/default.aspx. Accessed March 25, 2020.

Johari, J. C. (1997). *International Relations and Politics: Theoretical Perspectives*. New Delhi: Sterling Publishers.

Koops, B. (2016). "Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research." In Akhgar, B., & Brewster, B. (Eds.) *Combating Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*. Geneva: Springer.

Kosseff, J. (2017). *Cybersecurity Law*. Hoboken, NJ: John Wiley & Sons.

Kremling, J., & Parker, A. M. S. (2018). *Cyberspace, Cybersecurity and Cybercrime*. London: Sage.

Kshetri, N. (2019). "Cybercrime and Cybersecurity in Africa." *Journal of Global Information Technology Management* 22(2): 77–81.

Leffler, M. P. (1990). "National Security." *Journal of American History* 77(1): 143–153.

Lijphart, A. (1975). "The Comparable-Cases Strategy in Comparative Research." *Comparative Political Studies* 8(2): 158–177.

Mazurczyk, W., Drobniak, C., & Moore, S. (2016). "Towards a Systematic View on Cybersecurity Ecology." In Akhgar, B., & Brewster, B. (Eds.) *Combating Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*, 17–38. Geneva: Springer.

Maurer, T. (2018). *Cyber Mercenaries: The State, Hackers and Power*. New York: Cambridge University Press.

Maurushat, A. (2013). *Disclosure of Security Vulnerabilities: Legal and Ethical Issues*. Berlin: Springer.

Meeuwisse, R. (2015). *Cybersecurity for Beginners*. Canterbury, New Zealand: Icutrain Ltd.

Mohammed, K. H., Mohamed, Y. D., & Solanke, A. A. (2019). "Cybercrime and Digital Forensics: Bridging the Gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria." *International Journal of Cybersecurity Intelligence and Cybercrime* 2 (1): 56-63.

Mordi, M. (2019). "Is Nigeria Really the Headquarters of Cybercrime in the World?" *Guardian*. https://guardian.ng/news/is-nigeria-really-the-headquarters-of-cybercrime-in-the-world/. Accessed March 25, 2020.

Mowbray, T. J. (2013). *Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions*. Indianapolis, IN: John Wiley & Sons.

National Bureau of Statistics (2018). Nigerian Population Estimate. https://www.nbs.org.ng. Accessed March 25, 2020.

Noam, E. M. (2019). *Managing Media and Digital Organisations*. New York: Palgrave

Macmillan.

Ohwovoriole, O. (2019). "Nigeria Losses About N127bn to Cybercrime Annually." *ThisDay*. https://allafrica.com/stories/201906190144.html. Accessed March 25, 2020.

Olayemi, O. J. (2014). "A Socio-Technological Analysis of Cybercrime and Cyber Security in Nigeria." *International Journal of Sociology and Anthropology* 6(3): 116–125.

Omodunbi, B. A., Odiase, P. O., Olaniyan, N., & Esan, A. O. (2016). "Cybercrimes in Nigeria: Analysis, Detection and Prevention." *FUOYE Journal of Engineering and Technology* 1(1): 37–42.

Pelton, J. N., & Singh, I. B. (2015). *Digital Defense: A Cybersecurity Primer*. Cham: Springer.

Rayes, A., & Salam, S. (2019). *Internet of Things: From Hype to Reality*. Geneva: Springer.

Re-Hashed. (2019). *Cybercrime Statistics: A Closer Look at the "Web of Profit*. www.thesslstore.com. Accessed March 25, 2020.

Reveron, D. S. & Mahoney-Norris, K. A. (2011). *Human Security in a Borderless World*. New York: Routledge.

Rittinghouse, J. W., & Hancock, W. M. (2003). *Cybersecurity Operations Handbook*. Amsterdam: Elsevier.

SaharaReporters. (2019). "Nigerian Government Directs NCC to Block Over Nine Million Unregistered SIM Cards." http://saharareporters.com/2019/09/12/nigerian-government-directs-ncc-block-over-nine-million-unregistered-sim-cards. Accessed March 25, 2020.

Schjolberg, S., & Ghernaouti-Helie, S. (2009). *A Global Protocol on Cybersecurity and Cybercrime: An Initiative for Peace and Security in Cyberspace*. Oslo: E. Dit.

Schjolberg, S., & Ghernaouti-Helie, S. (2011). *A Global Treaty on Cybersecurity and Cybercrime*. Oslo: AiTO.

Schwanholz, J., & Graham, T. (2018). "Digital Transformation: New Opportunities and Challenges for Democracy." In Schwanholz, J. & Graham, T. (Es.) *Managing Democracy in the Digital Age: Internet Regulations, Social Media Use, and Online Civic Engagement*. Geneva: Springer.

Severo, M. (2019). "Safeguarding without a Record? The Digital Inventories of Intangible Cultural Heritage." In Romele, A., & Terrone, E. (Eds.) *Towards a Philosophy of Digital*

Media, 165–182. New York: Palgrave Macmillan.

Shalhoub, Z. K., & Al Qasimi, S. L. (2010). *Cyber Law and Cyber Security in Developing and Emerging Economies*. Northampton, UK: Edward Elgar.

Sharan, M. P. (2009) *Qualitative Research Method*. San Francisco: John Wiley & Sons.

Singer, P.W., & Friedman, A. (2011). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.

Sule, B. (2018). *Political Party Financing and Election Reformations in Nigeria's 2015 General Election: Issues and Impacts*. PhD Thesis submitted to the School of International Studies, College of Law Government and International Studies, Ghazali Shafie Graduate School of Government, Universiti Utara Malaysia.

Sule, B. Yahaya, M.A. Rabi'u, A.A. Ahmad, M. & Hussaini, K. (2019). "Strategies of Combating Insurgency in Northeastern Nigeria: A Non-Traditional Approach." *Journal of Administrative Studies* 16(2): 54–75.

Statista. (2019). "Nigeria: Number of Internet Users from 2017–2023 in Millions." https://www.statista.com/statistics/183849/internet-users-nigeria/. Accessed March 25, 2020.

Taylor, B. (2012). *The Evolution of National Security Studies*. Australian National University, National Security College Occasional Paper.

Touhill, G. J., & Touhill, C. J. (2014). *Cybersecurity for Executives: A Practical Guide*. Hoboken, NJ: John Wiley & Sons.

Walker III, W. O. (2009). *National Security and Core Values in American History*. Edinburgh, UK: Cambridge University Press.

Wolfers, A. (1964). *Discord and Collaboration: Essays on International Politics*. Baltimore: John Hopkins Press.

World Bank. (2017). *Combating Cybercrime: Tools and Capacity Building for Emerging Economies*. Washington, DC: World Bank.

Yakubu, Y. A. (2012). *Nigerian Foreign Policy from 1999–2012*. Zaria, Nigeria: Ahmadu Bello University Zaria Press.

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods*. London:

Sage.