JOURNAL OF POLITICAL DISCOURSE
ISSN Print: 2992-2763 – ISSN Online: 2992-4618 | Vol. 2, Issue 1, No. 2 / March 2024
https://www.jopd.com.ng

GLOBALISATION AND NATIONAL SECURITY: PERSPECTIVES ON CYBERSECURITY THREATS IN NIGERIA

Emmanuel Idemor Ukhami (Ph.D)
emmysunny@yahoo.com

Dahiru Abdulsalam (Ph.D)
abdulsalam38@yahoo.com

ABSTRACT

Globalization has led to a significant increase in the use of technology, making life easier by the day for individuals around the world to relate with each other and interconnect. However, it has also brought with it challenges that threaten national security. Cybersecurity threats are one of those challenges that have now constituted a major concern for nations worldwide. Nigeria, as a country, is not immune to these threats, and its national security has been affected by cyber-attacks. The paper highlights the various forms of cyber-attacks faced by the country, such as hacking, online fraud, identity theft, and cyber-terrorism. It also provides the historical antecedence of cybersecurity, factors precipitating cybersecurity threats, and implications of cybersecurity threats in Nigeria. It explores the measures put in place by the Nigerian government to address these threats. The paper also adopted the theory of Technology-Enabled Crime and employed the secondary source of data collection. Emphasis is made on the need for international cooperation to effectively combat cybercrime, particularly between Nigeria and nations with advanced technological capabilities. It also suggests the establishment of a central cybersecurity institution that will coordinate national cybersecurity affairs.

Keywords: Globalisation, National Security, Cybercrime, Cybersecurity, Threats.

Introduction

No doubt, the world has shrunk into a panorama of "connected space" and a time capsule; no nation-state can be in a state of autarky anymore. There is a binding force that has kept the nations of the world together. The force is globalisation. In the current era of globalisation, there is a dynamic interaction between and among nation-states and individuals (Agaba and Ukhami, 2015); hence, the buzzword - "global village." It is not arguable that globalisation has broken national barriers through the speed of technology, the proliferation of international organizations, and international economic relations, among others. Indeed, globalisation is a game changer. It has magnets the wider world into a complex whole and a holistic picture through easy accessibility, networking, communication, knowledge sharing and acculturation, and political and socio-economic interaction. Security which is the heart of human existence has been impacted by the forces of globalisation positively and negatively. While the international order among states is quite strong, according to Zalur and Zeckhauser (2002), the world is not peaceful. In the wake of globalisation and the explosion in communication technologies, new security-related threats have emerged that are to a great extent independent of national boundaries. As a result, a new kind of war is being waged in every country all over the world; this is because the primary threats to national security have changed fundamentally. They no longer spring from territorial and ideological disputes among nation-states but from how far globalisation, technological threats, and criminal networks have grown to challenge nation-states.

Indeed, the emergence of widespread security challenges in the global arena necessitates the rethinking of the foundation of contemporary global security (Buzan 1983, p.4). Cybersecurity, in particular, poses an unrelenting challenge, threatening the existence of mankind and infrastructures across nation-states. Countries are making serious efforts to protect their cyberspace from cyber-attacks 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). Scholars like Singer & Friedman (2014) have pointed out that the internet and cyberspace are global and pose multiple vulnerabilities to all nation-states.

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. Cybersecurity is often not critically focused on, but it has a significant impact on the economy and security of the nation. The country has seen a sharp increase in cyber-attacks in recent years, with businesses, government agencies, and even individuals being targeted. In Nigeria, the survey led by Gantz (2013) reveals that perpetrators of cyber-attacks entrench or implant counterfeit software with dangerous malware as a new technique of preying on computer users who are unaware of the potential danger. Therefore, indicating more danger to the computers of those who acquired counterfeit and pirated software. According to Ladipo (2022), a report on incidents of ransomware revealed that 71% of Nigerian organizations suffered cyber-attacks in 2021, with 44% of these organizations paying an average cost of $3.43 million as ransom to protect their business and secure sensitive data. According to Chukwuma and Mogom (2018), studies on cybersecurity, Nigeria is as vulnerable as other countries in the world. The country, as a result of rapid technology and access to information and the wider world, has faced the challenges of various kinds of cyber-threats in both cyberspace and cybersecurity such as hacking, yahoo-yahoo, and cyber-terrorism, among others.

The internet has facilitated dramatic increases in worldwide interconnectivity and communication. This form of globalisation has yielded benefits, such as improved living standards in the developing world, but it has also given rise to new weapons of resistance for groups seeking to oppose certain political measures and ideologies. Another instance that has posed a threat to the country's cyberspace according to Adigun (2012) is the Boko Haram terrorist group. "In August 2012, Boko Haram reportedly hacked the personnel records databases of Nigeria's secret service. The individual who successfully compromised the covert-personnel data system indicated the breach was executed in the name of Boko Haram and as a response to Nigeria's handling of interactions with the group". However, since its association with Al Qaeda, Boko Haram has demonstrated a vastly changed approach to executing its attacks. Attacks are now more violent and reflect the markings of training by al Qaeda personnel. Given that cyberspace has been part of the terrorists' warfare tool kit since 1998 when the Tamil Tigers executed a distributed denial of service attack, (Denning, 2000) and al Qaeda has used the internet as a vital communication vehicle since 1996, Boko Haram's incorporation of cyber into its arsenal is almost inevitable. Boko Haram's tactic advancement demonstrates that Nigeria and its neighboring Sahel region neighbors are ripe for exploitation as a cyber-warfare hub (Mills, 2009).

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. The recognition of this threat led to the adoption of a policy document on cybersecurity by the Nigerian government in 2014, a comprehensive policy statement detailing the provisions and efforts of the government aimed at achieving a safer digital environment. Yet, comprehensive analysis of Nigerian cybersecurity issues is woefully inadequate because of a lack of technological sophisticatedness, compromises within the cybersecurity infrastructures, and inadequate manpower with the prerequisite skills to manage cybersecurity in the country. The paper seeks to evaluate the impact of cybersecurity threats and the extent of securing cyberspace for Nigeria's national security.

Conceptual and Theoretical Framework

Globalisation

Globalisation is a multifaceted and multidimensional conception that is laden with ideological extrapolations depending on which aspect of the North/South divide one is viewing it from. This is manifest in the abundance of meanings that have characterized it (Saliu and Aremu, 2013). This is why the concept of globalisation is a slippery and indefinable one. Any attempt to define globalisation

would certainly prove contentions, complex and nebulous. A concept often discussed, but a seldom defined phenomenon, globalisation seems to defy any universally accepted orthodox definition.

According to Tar and Ukhami (2016), the diverse nature and interconnectedness of the world have made the concept of globalisation perhaps the most popular buzzword used by both Western and non-western countries alike. It is a bug that cuts across individuals, families, religions, and society.

According to Tar (2016), the world is increasingly becoming integrated and interdependent as a result of advances in information and communication technologies (ICTs), and changes in global economic and political spectrums. These days, we hear common references to concepts such as "global village", "wired world", "internet age", and "Twitter revolution". These concepts reveal that the world is now more connected. Globalisation has made it possible for remote parts of the world to be exposed to the wider world. It has also made it possible for highly developed regions/countries to access areas that have been hitherto less penetrable.

According to Stiglitz (2002, p.9), globalisation is the closer integration of countries… and the breaking down of artificial barriers to the flow of goods, services, capital, and people across borders. For instance, McGrew (2013, p.16) sees globalisation as simply the widening, deepening, and speeding up of worldwide interconnectedness. This view is in line with the definition given by Obadan (2004, p.3) of the increasing interconnectedness and interdependence among the worlds, regions, nations, governments, businesses, institutions, communities, families, and individuals.

Buttressing the above views, Afolayan (2002, p.33) conceives globalisation to be the intensification of global interconnectedness and interdependence which blurs national borders and policies in the shadow of global relations. Globalisation can also be seen as the phenomenon of increasing integration of nation-states through economic exchange, political configurations, technological advancement, and cultural influences. To Shodunke (2010), "globalisation deemphasizes national boundaries thus engendering greater movement of people, goods, capital, and ideas. Globalisation is like moving towards living in a borderless world." The foregoing definitions reveal that globalisation is a self-propelling networking process.

Globalization has led to technological breakthroughs such as mobile phones, computers, the internet, and satellite networks. Information and Communication Technology (ICT) has greatly impacted various sectors in Nigeria, including publishing, the health sector, financial institutions, entertainment, education, hospitality business, and social interactions. However, it should be noted that ICT has also had negative impacts on Nigerian society. According to Omekwu (2006), the more dangerous dimensions of the digital revolution include pornography, money laundering, cultism, international terrorism, and child abuse, which all pose a threat to African cultural heritage. It is challenging for African countries with strong Islamic and Christian cultures to tolerate the level of pornographic activities that occur on the internet. In traditional African culture, nudity is not considered a virtue, but in many African universities and urban centers, nudity has become commonplace, leading to the decline of Africa's rich and elegant dress styles. Additionally, globalization has contributed to the increase in arms proliferation, cyber-attacks, ethnic violence, global crime, and trafficking (Davis, 2003).

National Security

Security has been seen as a situation where a person or thing is not exposed to any form of danger or risk of physical or moral aggression, accident, theft, or deterioration. Some security experts argue that the concept of security has always been associated with the safety and survival of the state and its citizens from harm, destruction, or dangerous threats. Those conceptions generally hold that the state is the only institution with the primary responsibility and power for the safety of its territory and its people (Zabadi, 2005). The conclusion by Zabadi, brings us to the definition of national security, to extrapolate the role of the state to ensure the security of individuals, properties within the state, and of course the safety of the state itself.

The state plays a major role in the security of its citizens. Security is the key function of the state (Buzan, 2003). It emphasized the coercive means of putting all the aspects of the state in check. A nation can protect its national value from external threats. National security is seen in terms of a nation's military capabilities or the struggle to overcome internal and external aggression. A nation is secured once it is free from military threats or political coercion (Aliyu, 2012). National security has traditionally been about the state's survival against military threats posed by other states (Buzan,

2003). Security threat differs amongst nations. The major security threat to some powerful nations like the USA and its allies may be how to defeat international terrorists and promote their economic interests and democratic values (Aliyu, 2012). However, a nation like Nigeria has its peculiar security threat determined by socioeconomic and political circumstances. Thus, Nigeria's national security was outlined by former President Olusegun Obasanjo when he said:

> The primary objective of national security shall be to strengthen the Federal Republic of Nigeria, advance its interests and objectives, contain instability, enhance genuine development, progress, and growth, and improve the welfare, well-being, and quality of life of every citizen (Obasanjo, 2002).

National security refers to the capacity of the state to protect its interests/values from both internal and external threats. In essence, security is about the totality of policies and actions initiated and taken to protect the nation-state from both internal and external threats. To achieve a state of security states the world over, devise strategies and policy frameworks following the perceived threats to their citizens and properties (Essien, 2011).

Cyber-Security

The issue of cyber-security has recently caught the attention of some scholars because of the challenges of cyber-crime which is causing so much threat to nations' security. Though there is a paucity of literature on what the term means and how it is situated within various contexts, the subject matter has elicited various perspectives from scholars, and there is no definite definition of the subject matter. According to Kruse, Frederick, Jacobson, and Monticone, cyber security is a set of strategies and processes for defending computers, networks, databases, and applications against assaults, illegal access, modification, or destruction. It can also play a vital role in the development of information technology and Internet services. There are various trends in cyber security, the most prominent of which is Web applications. Web applications are now one of the most widely used platforms for delivering information and services via the Internet. Cyber security according to Kruse, Frederick, Jacobson, and Monticone (2017) refers to the technologies, techniques, and procedures that are used to prevent computers, programs, networks, and data from being hacked, damaged, or accessed without authorization.

According to Nwachukwu (2021), cybersecurity encompasses a set of policies, security concepts, tools, security safeguards, risk management approaches, guidelines, actions, best practices, training, assurance, and technologies that can be used to protect the cyber environment, organization, and user's assets. Organization and user assets include connected computing devices, personnel, applications, infrastructure, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security attempts to ensure the accomplishment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.

Cyber-security is the body of guidelines or templates put in place for the protection of cyberspace. But as individuals, organizations, and even states become more dependent on cyberspace, they undoubtedly face new risks. Cybercrime can also be referred to as a series of organized crimes attacking both cyberspace and cyber security. For instance, sophisticated cyber criminals and nation-states, among others, present risks to Nigeria's economy and national security. Nigeria's economic viability and national security depend on a vast array of interdependent and critical networks, services, systems, and resources known as cyberspace. Cyber-space has transformed the ways people communicate, travel, power their homes, run their economy, and obtain government services. Cyber-security is the body of technology, processes, and practices designed to protect networks, computers, programs, and data from attacks, damage, or authorized access (Maduagwu, 2005).

Nexus between Globalisation and National Security

There is a general agreement in the literature that there is a lucid link between globalisation and national security, but despite the plethora of literature on security and globalisation, there is relatively little work written by security specialists that interconnects the two, because both globalisation and national security are multidimensional constructs. According to Tor (2013, p.506), globalisation entails universalization whereby the object, practices, or even values transcends geo-political boundaries, penetrating the hitherto sovereign nation-state and impacting the orientation and value system of the people but especially national security.

Globalisation has progressively impacted cultural, economic, political and religious, and other forms of human social interaction, which plays very important roles at the international and national levels. Hence, globalisation and national security are linked as both have an influence on cultural, economic, political, religious, and other facets of human interactions and have also negatively or positively impacted the international system (David and Musa, 2016, p.511). Furthermore, globalisation is driven by technology, particularly transportation, and information and communication technology which have been used by terrorists globally and in developing countries like Nigeria threatening national development and security. Just as technology facilitates the speedy transfer of goods and services, information, and so on, generally, the extent of political, social, cultural, economic, and other forms of change brought about by globalisation such as increasing interconnectedness, interdependence, and homogeneity in the international system has an impact on development and national security. In increasing interconnectedness and interdependence of world economies, culture, politics, and other facets of social interaction, also created a gap in opportunities created by the interconnectedness. Hence, the increasing poverty, unemployment, underdevelopment, violent conflicts, and others in most parts of the world are manifestations of the negative impact on national security. So terrorism is one of those violent reactions to the various forms of interconnectedness brought by globalisation. As globalisation spreads and societies become increasingly interconnected, the national government's capacity to ensure national security is undermined and terrorism a manifestation of some of the negative forms of interconnectedness poses even more challenges for national security (David and Musa, 2016, p.511).

The arms proliferation, cyber-attacks, ethnic violence, global crime, and trafficking are occurred by globalisation (Davies, 2003). Globalisation is blamed for a host of other ills such as underdevelopment, violent conflicts, piracy, terrorism, etc, confronting the international community and national governments in the contemporary world. It is within this line of argument that globalisation as a process driven by technology, and specifically technological innovation and products such as motorcycles, cars, cellular phones, AK-47 guns, and others have contributed to and aided insecurity in Nigeria, such as Boko Haram terrorism, banditry, armed robbery and other forms of national security challenges. It is worth noting that, in Nigeria, just as in other third-world countries of the world, there is massive disintegration of national security as a result of globalisation.

The Theory of Technology-Enabled Crime (TEC)

The Theory of Technology-Enabled Crime is a criminological framework that seeks to explain how advances in technology have enabled new forms of crime. TEC is based on the premise that technology, while it has made our lives easier, has also created new opportunities for criminal behavior. The rise of the internet and other digital technologies has created a borderless world where people can connect and share information at the click of a button. This has made it easier for criminals to operate across national borders and has created new opportunities for crime. Cybercrime, which is the use of computers and the internet to commit crimes, has become one of the fastest-growing areas of crime in the world.

Some of the early work on the theory can be traced back to the 1990s, with the emergence of the internet and the growing use of computers in criminal activities. The exact date when the Theory of Technology-Enabled Crime was propounded is unclear, as it has been developed over time through the work of various researchers and scholars. However, McQuade (2006) is one of the most prominent scholars who emphasize the relevance of Technology-Enabled Crime theory with the growth in the

telecommunication industry. He notes that it encompasses such crimes committed directly against computers and computer systems which are often referred to as high tech crime, computer crimes, or cybercrimes. He reasons that the use of the Internet or technology helps to facilitate the commission of traditional crimes and it can take the form of fraud, scams, threats, and harassment which introduces multidimensional challenges to overcoming old crimes.

McQuade (2006) argues that technology-enable crime theory encompasses: 1. Crimes committed directly against computers and computer systems. 2. Activities that fall under this category are often referred to as high-tech crimes, computer crimes, or cybercrimes. 3. The use of technology to commit or facilitate the commission of traditional crimes. 4. Crimes such as fraud, scams, and harassment can be facilitated using technology which brings unique challenges to old crimes. The theory provides a framework for understanding all forms of criminality especially those that are evolving with computing and telecommunications technology inventions and innovations.

The Theory of Technology-Enabled Crime is particularly relevant to cybersecurity in Nigeria, as the country has seen an increase in cybercrime over the years. Terrorists now adopt information technology in raising funds, mobilizing supporters or recruiting, planning attacks, and monitoring security agencies to present the government as incapable of handling the situation. This weakens the citizenry's moral support for the government and the resolve of the security agencies striving to curb terrorist criminalities. Also, it is no surprise that online advance fee fraud, identity theft, financial/investment scam, phishing, employment scam, and others arise as opportunities for illegality within Nigeria's Global Information Infrastructure. In Nigeria, cybercrime has become a significant challenge to the country's economy and security. Hence, while technological development has more advantages than disadvantages, the theory points to the threats posed by emerging forms of cybercrime, transnational crime, and terrorist networks that defy traditional methods of criminal justice and security measures for preventing and controlling crimes.

Cybersecurity Incidence in Nigeria

Similar to other developing countries, the level of development in the internet and cyberspace in the 1970s and 1980s in the 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 an average of 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). The history of cybersecurity in Nigeria is relatively recent, as the country only began to develop its cybersecurity infrastructure in the early 2000s. Some of the most notable cybersecurity incidents in Nigeria include the following:

Hacking: one of the most challenging incidents to Nigeria's cybersecurity is hacking. For instance, there have been alleged hacks on governmental institutions/agencies in 2020, it was alleged that the website of the Central Bank of Nigeria – responsible for regulating the country's financial sector – was hacked by "Anonymous", a group of foreign Internet activists protesting police brutality in the country (Alfred, 2020). The group had earlier announced its decision to attack government websites in solidarity with the protesters who are calling for reform of the Nigerian police force. Although the CBN later debunked this report stating that its website was not hacked, this incident highlights the vulnerability of Nigerian businesses to cybersecurity attacks. In the same vein, there were other alleged attacks by Anonymous on other government-owned institutions/agencies including the Economic and Financial Crimes Commission (EFCC), Independent National Electoral Commission (INEC), National Broadcasting Commission (NBC), Nigeria Police Force, Nigeria Stock Exchange, and several others (Alao, 2020). Also, in 2019, the Joint Admissions and Matriculation Board

(JAMB) reported that its website was hacked and the personal data of millions of students was compromised.

According to The Guardian Newspaper report in August 2021, a certain Salau Abdulmalik Femi, a Nigerian man, was arrested by detectives from the Special Fraud Unit (SFU) of Nigeria Police Force (NPF), for allegedly hacking into the server of a Nigerian bank and stealing N1.87 billion (guardianng, 13 August 2021). The suspect is said to be the kingpin of a syndicate with criminal expertise in hacking into the servers of banks and corporate agencies. This story highlights just how easy it is for criminals to commit fraud - with users' personal and financial information online, and steal large sums of money using technology. Reportedly also, a Nigerian hacker known as Ihebuzo Chris demonstrated that the security measures in place around the Access Bank network are not as effective as they should be (Unini, 2020). The hacker, who referred to himself as a python on Twitter, was able to gain access to the data of over 2,000 customers and extracted sensitive information such as their BVN numbers, account numbers, and other details. In a viral video that was circulated online, Chris showed the printout of the customer accounts that he was able to access, highlighting the ease with which he was able to do so… (Guardian, 1 February 2022).

Online Fraud: Cybercrime is a significant problem for Nigeria, causing both concern and embarrassment for the nation. While the Internet provides unlimited opportunities for commercial, social, and educational activities, it also introduces peculiar risks. From fake lotteries to massive internet scams, Nigeria has experienced a range of cybercrimes. For instance, Elekwe, a 28-year-old man with a diploma in computer science, made a fortune through scamming after being lured to Lagos by the chief of a fraud gang at a business center. Despite being jobless for two years, Elekwe now owns three sleek cars and two houses from his exploits. In July 2001, security agencies arrested four Nigerians suspected of operating a "419" scam on the internet to dupe unsuspecting foreign investors in Ghana, leading to the loss of millions of foreign currencies by prospective investors. In another case, Mike Amadi was sentenced to 16 years in prison for setting up a website that offered phony procurement contracts, impersonating the EFCC Chairman. He was caught by an undercover agent posing as an Italian businessman.

The biggest international scam was committed by Amaka Anajemba, who was sentenced to 2½ years in prison and ordered to return $25.5 million of the $242 million she helped steal from a Brazilian bank. These instances of cybercrime have caused a traumatic image for Nigeria, and it is essential to strengthen cybersecurity measures to mitigate the risks associated with the internet.
In 2020, Ramon Abbas, also known as "Hushpuppi", a popular Instagram personality known for his lavish lifestyle, was arrested in Dubai and extradited to the United States on charges of fraud and money laundering. He was accused of being part of a network that stole millions of dollars from individuals and companies around the world. These are just a few examples of reported cases of online fraud in Nigeria or done abroad by Nigerians.

Malware: these attacks are a common form of cyber threat in Nigeria, and they occur in various forms. Here are some examples of reported cases of malware attacks and where they occurred in Nigeria:

In 2017, the WannaCry ransomware attack affected over 200,000 computers in 150 countries worldwide, including Nigeria. The malware infected the computer systems of several Nigerian organizations, including the Nigerian National Petroleum Corporation and the Nigerian Ports Authority. In the same year, the Petya ransomware attack affected computer systems worldwide, including Nigeria. The malware infected the computer systems of several Nigerian organizations, including the Lagos State Government and the Dangote Group.

In 2018, it was reported that a group of hackers had used spyware to monitor the computer systems of Nigerian government officials. The spyware was used to steal sensitive information and gain access to the officials' email accounts. That same year, it was reported that a group of hackers had used malware to target ATMs in Nigeria. The malware was used to steal sensitive information and cash

from the machines. In 2020, it was reported that the Emotet malware had infected several computer systems in Nigeria. The malware was used to steal personal information and spread other types of malware, including ransomware.

Cyber-terrorism: there have been some reported incidents of cyberterrorism in Nigeria, but the number is relatively low compared to other countries. Cyberterrorism refers to the use of technology to conduct acts of terrorism; such as attacks on critical infrastructure or government systems. One notable incident of cyberterrorism in Nigeria occurred in 2016 when a group of hackers claiming to be part of the Islamic State (ISIS) targeted the website of the Nigerian Army and released a list of senior army officers along with their personal information. However, the Nigerian government downplayed the incident, stating that it was not a significant threat. Another incident occurred in 2018 when a group known as "the Turkish Cyber Army" claimed responsibility for a series of attacks on Nigerian government websites. The group reportedly defaced several websites and leaked sensitive information, including the personal details of government officials.

The integration of technology in the operational plan of Boko Haram has by no means aided their striking power and assisted them in the exchange of information, recruitment, ideological propagation, training, and finances through electronic transfers. In addition, it has occasioned traumatic experiences on the part of the citizenry and the general belief that the government has been incapable of curtailing them.

Phishing: these attacks are a common form of cyber threat in Nigeria and occur in various forms, including email, SMS, and social media. There are some examples of reported cases of phishing attacks and where they occurred in Nigeria. For instance, in 2019, it was reported that a Nigerian woman had fallen victim to a job scam after responding to an advertisement on social media. The scammer had requested that she pay a fee to secure the job and had then disappeared after receiving the payment. In the same year, it was reported that a Nigerian bank had fallen victim to an email phishing scam that resulted in the loss of N3.5 million ($9,700) from its account. The scammer had sent an email posing as a representative of one of the bank's foreign partners and requesting a funds transfer. Eleanya (2021) reported that in 2020, Nigerian banks lost N3.5 billion between July and September 2020 to fraud-related incidences, representing a 534-percent increase from the same period in 2019, when it was N552 million.

In 2020, it was reported that a man in Lagos fell victim to a phishing scam that resulted in the loss of N500,000 ($1,400) from his bank account. The scammer had sent him an email posing as his bank and requesting that he update his personal information.

Factors Precipitating Cybersecurity Threats in Nigeria

Cyberspace crime and criminality are motivated by several factors in Nigeria. Some of these factors are as follows:

Sheer Curiosity: contribute to cybersecurity threats in Nigeria. Curiosity is a natural human trait, and some individuals may be tempted to explore and experiment with technology and software without understanding the potential consequences of their actions (Nwaogu, 2018). For instance, some individuals (especially young people) may engage in activities such as hacking, cracking, or penetration testing out of curiosity without realizing that these activities are illegal and can have serious legal consequences. Moreover, some individuals may engage in social engineering techniques, such as phishing, to obtain personal or sensitive information about others, out of sheer curiosity or for personal gain. Furthermore, curiosity can lead to the dissemination of fake news, misinformation, and propaganda, which can have serious consequences for individuals, organizations, and even the country as a whole. This can lead to the spread of rumors and false information that can damage reputations, cause panic, and incite violence.

Mischievousness: has been identified as one of the root causes of information security incidents in organizations (Safa, Maple, Waston, and Solms, 2018). The act of mischief-making is an agelong

phenomenon and as such not new. Mischief makers may employ the Internet as a tool to execute their nefarious activities. This is because the Internet can grant them relative anonymity. Mischief makers who could be current or former employees of an organization, political opponents, and former friends of the victim may target an organization or an individual for cyber victimization to get even for a perceived wrong. Furthermore, mischievousness can lead to the dissemination of false information or rumors, which can cause harm to individuals or organizations. This can lead to reputational damage, loss of business, or even harm to the country's image.

Unemployment: can contribute to cybersecurity threats in Nigeria. The lack of job opportunities can drive individuals to engage in cybercrime as a means of making a living. According to the National Bureau of Statistics (NBS) Nigeria's unemployment rate increased from 14.2% in Q4 2016 to 16.2% in Q2 2017 and 18.8% in Q3 2017 (National Bureau of Statistics, 2017). Again, in 2020 the National Bureau of Statistics, reported that "Nigeria's unemployment rate was 33.3% in the fourth quarter of 2020, which is one of the highest rates in the world" (National Bureau of Statistics, 2021).

It is argued that employment prevents crime for some people under certain conditions and that employment and criminality relate to each in several ways not only at the aggregate level but also at the individual level. Nigeria has an unemployment problem. The unemployment rate has been identified as one of the factors responsible for youth involvement in cybercrime (Ndubueze, 2017). Some unemployed youth in Nigeria are said to be involved in online advanced fee fraud (yahoo-yahoo) (Adeniran, 2008).

Poverty: can be a factor that contributes to cybersecurity threats in Nigeria. The lack of access to basic necessities, such as food, shelter, and education, can drive individuals to engage in cybercrime as a means of survival. According to a report by the World Bank, "Nigeria has one of the highest poverty rates in the world, with over 70% of the population living below the poverty line" (World Bank, 2021). The poverty and crime nexus has long been argued in criminological discourses.

On the other hand, poverty can lead to a lack of investment in cybersecurity infrastructure and personnel, leaving organizations and individuals vulnerable to cyber threats. According to a report by the Global Cybersecurity Index (GCI), "Nigeria has a low level of investment in cybersecurity infrastructure, which can make it difficult for organizations to protect themselves against cyber threats" (ITU, 2020). In addition, poverty can limit access to technology and the internet, which can make it difficult for individuals and organizations to stay up-to-date on cybersecurity best practices and emerging threats. This can leave them vulnerable to cyberattacks.

Quest for Wealth: can also be a factor that contributes to cybersecurity threats in Nigeria. Cybercriminals may engage in illegal activities such as hacking, phishing, and identity theft to make money quickly. The "get rich quick syndrome" is a driver for all kinds of crimes including cybercrimes. According to a report by the Nigerian Communications Commission (NCC), "many young people in Nigeria are attracted to cybercrime as a means to acquire wealth quickly" (NCC, 2020).

The desire for wealth and financial gain can also lead individuals and organizations to engage in cybercrime. For example, some companies may engage in cyber espionage or intellectual property theft to gain a competitive advantage in their industry. According to a report by the World Economic Forum (WEF), "Cybercrime is often motivated by financial gain, as criminals seek to steal valuable information or extort money from victims" (WEF, 2020).

Value Crisis: when there is a lack of ethical values and social responsibility, individuals and organizations may engage in cybercrime without considering the negative consequences. For instance, the rise in cyber fraud in Nigeria has been attributed to a lack of ethical values and social responsibility among some individuals and organizations. According to a report by the Central Bank of Nigeria, "cyber fraud has been on the increase in Nigeria due to the absence of ethical values among some of the perpetrators" (Central Bank of Nigeria, 2020). The undue emphasis on wealth accumulation has been linked to the involvement of Nigerian youths in online fraudulent practices (Adeniran, 2008).

Porous Nature of the Internet: the Internet is free for all with no central control. Hence, the state of anarchy is presently experienced. The internet provides an open and global platform for communication and exchange of information, but this can also create opportunities for cyber attackers to access networks and devices from anywhere in the world (Federal Trade Commission, n.d.). For instance, the use of unsecured or public Wi-Fi networks can make it easier for cyber attackers to intercept sensitive data and gain unauthorized access to networks and devices. Additionally, the use of social media platforms and other online services can provide cyber attackers with information about individuals and organizations that they can use for targeted attacks.

Lack of Strong Cyber Crime Laws: weak laws and regulations refer to the lack of effective legal frameworks and policies that govern cybersecurity practices in Nigeria. This can create an environment where cybercriminals can operate with impunity, knowing that there are few consequences for their actions. A study conducted by the International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) found that "the absence of cybersecurity laws and regulations in Nigeria has contributed to the rise of cybercrime" (Ajayi et al., 2021). Furthermore, the lack of clear definitions and guidelines for cybercrime in Nigeria's legal system can make it difficult to prosecute cybercriminals. According to a report by the Global Cybersecurity Index (GCI), "Nigeria's legal framework for cybersecurity is weak and does not provide adequate protection for citizens and critical infrastructure" (ITU, 2020).

Lack of Standards and National Central Control: the lack of standards and national central control is another factor that can contribute to cybersecurity threats in Nigeria. Without a centralized approach to cybersecurity, there may be inconsistencies in the way that organizations and individuals approach cybersecurity, leaving them vulnerable to cyber threats. According to a report by the Global Cybersecurity Index (GCI), "Nigeria does not have a national cybersecurity strategy or a national computer emergency response team (CERT), which means that there is no central point of coordination for cybersecurity activities" (ITU, 2020). This lack of central coordination can make it difficult to respond effectively to cyber threats and can leave critical infrastructure and individuals at risk.

Impact of Globalisation on Cybersecurity and Nigeria's National Security

The emergence of cyberspace, a virtual global domain, is increasingly impacting almost every aspect of man's life. The domain is transforming our economy and security posture more than ever before, creating opportunities for innovations and means to improve the general welfare of citizens. It is transforming many countries' growths, dismantling barriers to commerce, and allowing people across the globe to communicate, collaborate, and exchange ideas. Globalisation has brought about some positive impacts on cybersecurity and Nigeria's national security. Some of these impacts are global collaboration and cooperation, increased access to cybersecurity resources, enhanced cybercrime investigation and prosecution, increased awareness and education, improved access to technology, and increased investment in cybersecurity.

While there are positive impacts of globalization on national security, the Nigerian cybersecurity landscape is facing a range of challenges, including cybercrime, cyber espionage, and cyber terrorism which have significant implications for the country's national security. The country has become a prime target for cybercriminals, who take advantage of the low levels of cybersecurity awareness among citizens and organizations (Adeniran, 2019). The consequences of globalisation on cybersecurity and Nigeria's national security have an overwhelming effect. Some of these are increased cybersecurity threats, greater dependence on technology, cybersecurity skills shortage, cybercrime as a global business, collapse of national infrastructure, loss of finance, loss of the country's reputation, increased threat to national security, increasing vulnerability of citizens, contravene the territorial integrity of the state, and easy spread of terrorism.

Measures by the Government to Address Global Cybersecurity Challenges in Nigeria

However, while the impact of globalisation on the Nigerian cybersecurity threat landscape is undeniable, it is important to recognize that the country has made progress in addressing the challenges. Osho & Onoja (2015) argue that cybersecurity is a crucial issue that requires the utmost attention from governments, policymakers, and stakeholders, amidst several other existing government concerns. The importance of cybersecurity is gaining global attention, and it is imperative to craft guiding principles in the form of policies and strategies to govern cybersecurity issues carefully. As a result, concerned stakeholders must approach cybersecurity considerations cautiously to ensure that they are adequately addressed.

The Nigerian government has taken steps to strengthen its cybersecurity infrastructure. In December 2014 Nigeria published its National Cyber Security Strategy which mapped out Nigeria's National Cyber Security Vision and the strategies for achieving this vision (it was reviewed in 2021 to meet present realities). Furthermore, in May 2015, the President of the Federal Republic of Nigeria signed into law the Nigeria Cybercrime (Prohibition, Prevention, etc.) Act.

Other agencies of government like the National Information Technology Development Agency (NITDA) have also taken some precautionary measures to address the scourge of cybersecurity threats in Nigeria. Some of these are the National Cybersecurity Awareness and Safety Initiative in 2014 and the Nigeria Data Protection Regulation in 2019. Some of the institutions that have played a role as partners of the government in addressing cybersecurity threats in Nigeria include the Office of the National Security Adviser (ONSA), the Nigerian Communications Commission (NCC), the Economic and Financial Crimes Commission (EFCC), the Nigerian Police Force Cybercrime Unit (NPFCU), the National Cybersecurity Centre (NCSC), the Nigerian Computer Emergency Response Team (ngCERT), the Central Bank of Nigeria (CBN), the Department of State Security (DSS), Cybersecurity and Digital Forensics Institute of Nigeria, Federal Ministry of Communications and Digital Economy, among others.

Despite the positive impact of cybersecurity laws and institutions in Nigeria, there are still some challenges that require immediate interventions. These challenges include the rapidly increasing number of internet and computer users, lack of dedicated cybersecurity agencies, poor performance of law enforcement agencies, technological sophisticatedness, lack of awareness, lack of investment in cybersecurity, and lack of skilled personnel.

Conclusion and Recommendations

There is no doubt that the globalisation of the world has brought with it opportunities such as increased trade, investment opportunities, and improved technology. However, it has also exposed countries to various security threats, particularly in the realm of cybersecurity and Nigeria is not immune to these threats. Globalisation indeed has a strong influence on national security.

The surfing of the internet with a view of getting information, processing, retrieving, saving, and downloading, has led to all forms of cybersecurity threats including cybercrimes, cyberterrorism, and cyber espionage. In Nigeria, cyber insecurity has become rampant with several precipitating factors contributing to increasing cyber threats such as growing unemployment and quick-to-getrich motive, and lack of adequate cybersecurity policies, regulations, and technical capabilities to effectively detect, prevent, and respond to cyber-attacks.

Though the Nigerian government has taken several measures to address cybersecurity challenges in the country (which are commendable), cybercriminals (from within and outside the country) keep devising new technology to perpetuate their nefarious crime against individuals and national critical infrastructure in Nigeria. Therefore, more needs to be done to address cybersecurity challenges in Nigeria such as creating a central cybersecurity agency solely responsible for national cybersecurity with the needed cybersecurity infrastructure and technologies to coordinate other agencies in the area of cybersecurity. The Nigerian government must also deal with the identified causes of cyber threats, and finally, Nigeria can leverage international partnerships to build cybersecurity capacity and exchange best practices with other countries since cybersecurity is a global issue.

References

Adeniran, A.I. (2008). "The Internet and Emergence of Yahoo-Boys Sub-Culture in Nigeria." *International Journal of Cyber Criminology*. 2 (2): 368–381.

Adeniran, O. (2019). "Cybersecurity and the Nigerian Economy: Challenges and Prospects." *Journal of Internet Banking and Commerce.* 24(2), 1-8.

Adigun, (2012). "AP Exclusive: Nigeria Secret Police Details Leaked." Salon, August 30, 2012, http://www.salon.com/2012/08/30/ap_exclusive_nigeria_secret_police_details_leaked/.

Afolayan, A. (2002). *Political Concepts and Ideologies: Nationalism and the Nation State*. Hope Publications.

Agaba, H. and Ukhami, E. (2015). *Issues in International Relations*. True Image Global Resources.

Ajayi, I.A., Oluwasegun, A., Adeola, O., & Adekunle, Y. (2021). "Cybersecurity Governance in Nigeria: Legal Framework, Challenges, and Prospects." *International Journal of Advanced Research in Computer Science and Software Engineering*. 11(2), 1-9.

Alfred, O. (2020). "#EndSARS: Anonymous attacks CBN website." *Premiumtimesng,* 16 October

Aliyu, B.M. (2012). "The Search for National Security in Nigeria: Challenges and Prospects." *Public Lecture Organized by the Obafemi Awolowo Institute of Government and Public Police*. Lagos: The Agip Reck Hall.

Antonucci, D. (2017). *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*. 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

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

Buzan, B. (1983). *Peoples, States and Fear. The National Security Problems. In International Relations.* Addison Wesley: Longman.

Central Bank of Nigeria. (2020). *Cyber Fraud in Nigeria*. Retrieved from https://www.cbn.gov.ng/Out/2020/FPRD/Cyber%20Fraud%20in%20Nigeria.pdf

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.

David, N.A and Musa, A. (2016). Globalisation, Insurgency and Mobility: The Impact of Ban on Motorcycle Transport in Adamawa State, Nigeria. In Tar, U.A., Tedheke, M.E.U. and Mijah, E.B. (eds). *Readings on Globalisation and Development in Africa.* Nigerian Defence Academy Press.

Davis, E.L. (2003). "Globalisation Security Implications." *RAND Issues Paper.*

Essien, F. (2011). "Management of Security Threats in Nigeria: An Interactive Approach." In Albert, I., Eselebor, W. and Danjibo, N. (eds.). *Peace Security and Development in Nigeria.* John Archers.

Federal Trade Commission. (n.d.). *Internet of Things (IoT).* Retrieved from

https://www.ftc.gov/tips-advice/business-center/privacy-and-security/internet-things-iot

Gantz, J. (2013). "One in Three PCs Risks Cyber-Attack in 2013." *Punch Newspapers.* Lagos, March 7, p. 14.

Guardian Nigeria (2022). "How we Apprehended Access Bank's Account Hacker – EFCC." 1 February.

Guardianng, (2021). "Man Hacks into Nigerian Bank's System, Steals N1.87 Billion." Editor. 13 August

ITU. (2020). "Global Cybersecurity Index 2020." *Nigeria Country Report*. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2020-PDF-E.pdf

Kruse, B., Frederick, T.J. and Monticone, D.K. (2017). "Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends." *Tech. and Health Care*. Vol. 25, no. 1, pp. 1-10, 2017

Ladipo, E. (2022). "Ransomware attacks Hit 71% of Nigerian Organizations with most Paying Ransom." *Businessday*. 3 May

McGrew, A. (2013). "Globalisation and Global Politics." In Baylis, J., Smith, S. and Owens, P. (eds.). *The Globalisation of the World*. Oxford University Press.

McQuade, S. (2006). *Understanding and Managing Cybercrime*. Allyn & Bacon.

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

National Bureau of Statistics (2017). *Unemployment and Underemployment Report*. Retrieved April 22, 2017 from nigerianstat. gov.ng/download/694.

National Bureau of Statistics. (2021). *Labor Force Statistics: Unemployment and*

Underemployment Report. Retrieved from https://www.nigerianstat.gov.ng/download/796

NCC. (2020). *Cybersecurity Awareness: NCC Raises Alarm over Youths' Involvement in Cybercrime*. Retrieved from https://www.ncc.gov.ng/media-centre/news-headlines/774cybersecurity-awareness-ncc-raises-alarm-over-youths-involvement-in-cybercrime

Ndubueze, P.N. (2017). "Cyberterrorism and National Security in Digital Nigeria." In Adejoh, P.A. and Adisa, W. (eds.). *Terrorism & Counter Terrorism War in Nigeria: Essays in Honour of Lieutenant General Tukur Yusuf Buratai*. pp. 325-247. University of Lagos Press.

Nwachukwu, (2021). "Nigeria: A Failing State Teetering on the Brink." *The Punch News.* 19 May.

Obadan, I.M. (2004). *Globalisation and Economic Development in Africa. In Globalisation and Africa's Development.* The Nigerian Economic Society.

Obasanjo, O. (2002). *Grand Strategy for National Security*. Abuja.

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

Omekwu, C.O. (2006). African Culture and Libraries: the Information Technology Challenge. *The Electronic Library*, 24 (2), 243-264.

Osho, O., & Onoja, A. (2015). "National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis." *International Journal of Cyber Criminology* (IJCC), 9(1), 120 - 143. doi:001:10.5281/ZENODO.22390 Nigeria: Data Privacy Regulations under the Nigerian Data Protection Regulation

Safa, N.S., Maple, C., Watson, T. and Sloms, R.V. (2018). "Motivation and Opportunity Based Model to Reduce Information Security Insider Threats in Organizations." *Journal of Information Security and Applications*. https://doi.org/10.1016/j.jisa.2017.11.001

Saliu, H., and Aremu, F.A. (2013). *Introduction to International Relations*. College Press and Publishers Limited.

Shodunke, O.A (2010). "Globalisation and National Security: Challenges for Nigeria." *A Research Project Submitted to National Defence College*. Nigeria, August

Stiglitz, J. (2002). Globalisation and its Discontent. Penguin Books Limited.

Tar, U.A. (2016). "Globalisation and New World Order: A Critique of Emerging Global Agenda and Implications for Africa and the Global South." In Tar, U.A., Tedheke, M.E.U. and Mijah, E.B. (eds). *Readings on Globalisation and Development in Africa.* Nigerian Defence Academy Press.

Tar, U.A. and Ukhami, E. (2016). "Globalisation and Development of Sports in Africa: Level Playing Field or Arena of Inequality?" In Tar, U.A., Tedheke, M.E.U. and Mijah, E.B. (eds). *Readings on Globalisation and Development in Africa.* Nigerian Defence Academy Press.

Tor, J.T (2013). "Globalisation and Nigeria's National Security: A Discourse on Contending Issues." In Mbachu, O. and Bature, U.M. (eds). Internal Security Management in Nigeria: A Study in Terrorism and Counter-Terrorism. Medusa Academic Publishers Limited.

Unini, C. (2020). "Access Bank Computers Leaking, Hacker Ihebuzo Steals Customers Data." *Thenigerialawyer*. 1 September

WEF. (2020). *Cybercrime: The Dark Side of the Internet.* Retrieved from https://www.weforum.org/agenda/2020/06/cybercrime-dark-side-internet/

World Bank. (2021). *Nigeria Overview*. Retrieved from https://www.worldbank.org/en/country/nigeria/overview

Zabadi, S.I. (2005). *Understanding Security and Security Sector Dynamics.* John Hopkins University Press.