CYBERSECURITY, PROLIFERATION, CHALLENGES AND SOLUTIONS

(A CASE STUDY OF THE NIGERIA STATE)

by

Matthew Erumusele Okoromi

(Nottingham, United Kingdom; princematt2000@gmail.com)

Abstract

With increasing access to internet and online resources in Nigeria, an exponential increase is observed in the rate of cybercrimes in Nigeria. Cybercrime rates increase geometrically, hence, giving Nigeria notoriety as a nation with a highly insecure cyberspace. In this Seminar Paper as a Subject Matter Expert (SME) with over 19 years wealth of knowledge and experience, I will be highlighting some of the most pressing contemporary challenges in cybersecurity as it affects the management of contemporary complex security challenges in Nigeria and to offer recommendations and solutions for the future. And as internet connectivity continues to spread, my belief is that this Seminar Paper will offer readers greater awareness of the threats of tomorrow—and serve to inform public debate into the next information age.

Introduction

Nigeria like several other countries across the globe is currently witnessing a surge in digital digital transformation. Many activities are now migrating to the internet especially with advent of covid-19 pandemic and the emergence of new technologies. Consequently, Nigeria cyberspace has become a centre-stage for new business innovations, government functions, and social interactions. This trend has created an opportunity for the country to realign it priorities and articulates effort towards attaining of national objectives. The current attributes of cyberspace also pave the requisite path for the adoption of technologies, dismantling of barriers to commerce, reinforcement of economic posture and enhancement of seamless competition across borders. The opportunities offered by cyberspace revolution also creates a platform for the enhancement of effective synchronization of effort of intelligence, security and defence communities towards addressing the mirage of security challenges confronting the country.

However, the increased dependence on cyberspace comes with risk that have significant national security and economic implications. The dynamic nature of cyber threats and the constantly evolving tactics of perpetrators of cybercrime pose serious risks to business, commercial and financial activities which are all now extensively reliant on cyberspace. These cyber threats also constitute hazards to everyday user of cyberspace which cut across government establishments, private sector and the general populace. Furthermore, these threats have the potential to compromise critical network systems leading to distortions of essential services. In most cases these disruptions are created by individuals or group using arrays of malicious activities and attack motivated by financial gains, anti-government or terrorist related activities thus challenging the confidentiality, integrity and availability (CIA) of data in Nigerian cyber space.

In a bid to address these multi-faceted cyber threats and embolden the country for efficient and progressive use of cyber domain the Federal Government of Nigeria (FGN) through the Office of National Security Adviser (ONSA), undertook several practical steps to draw the necessary cybersecurity roadmap for Nigeria. In this light, the National Cybersecurity Policy and Strategy 2014 was developed to provide direction for the mainstream Nigerian's National Cybersecurity Program and set the path for effective coordination of activities of all relevant stakeholders across government, academia and the private sector to handle the dynamism of security threats in the cyber domain. The Cybercrimes (Prohibition, Prevention etc.) Act 2015 was also developed and signed into law as the legal and regulatory framework for implementation and governance of national cybersecurity in the country. However, in view of emergent nature of cyber threats as well as constantly evolving technological and socio-economic imperative that depends on cyber domain, provisions were made for the review of the national cybersecurity policy and strategy every 5years in line with global best practices. The focus was also to hinge on the significant progress in cybersecurity made by the country between 2014 and 2021 while also realigning the efforts with objectives of Nigeria's National Security Strategy 2019.

Cybersecurity and Cybercrime in Nigeria

The words Cybersecurity and Cybercrime are used interchangeably. Computer crime can broadly be defined as criminal activity involving an information technology infrastructure: including illegal access or unauthorized access; illegal interception that involves technical means of non-public transmissions of computer data to, from or within a computer system; data interference that include unauthorized damaging, deletion, deterioration, alteration or suppression of computer data; systems interference that is interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data; misuse of devices, forgery (ID theft), and electronic fraud. The advent of digital technology gave birth to modern communication hard-wares, internet service and powerful computer systems to process data. Hence, cyberspace has provided a safe haven for internet platform, which has created geometric growth and accelerated windows of opportunities for businesses and the removal of economic barriers hitherto faced by nations of the world. People from diverse areas of human endeavour can now freely access and utilize the advantages offered by internet platform. However, information technology revolution associated with the internet in Nigeria has brought about a new wave of crime. A very few criminally minded youths in the country, who are mostly not educated or graduates, are stealing and committing atrocity through the aid of the internet online business transactions. The internet online business services, which ordinarily supposed to be a blessing as it exposes one to a lot of opportunities in various field of life is fast becoming a source of discomfort and worry due to the atrocity being perpetrated through it. Cybercrime has come as a surprise and a strange phenomenon that for now live with us in Nigeria. Computer crimes encompass a broad range of potentially illegal activities. Generally, it may be categorized into two major groups: (1) crimes that target computer networks or devices directly; (2) crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device. Nigeria was recently identified as the innocent and ignorant passive player in cyberspace knowledge Olympiad. The capture of Al Qaeda's operative, Muhammad Naeem Noor Khan, provided the Pakistani and American Intelligence Authority with some of Al Qaeda's Internet

Communication Strategy. It also identified that Nigerian Websites and Email System were used by Al Qaeda to disseminate internet information. This has once again brought up the pertinent questions of the safety and security of Nigeria's national cyberspace. This paper therefore addresses issues that deals with cybercrime based on false pretence or impersonation. An area that is likely to be fertile to the cyber criminals also called "yahoo boys" is the stock exchange market. Proper mechanism needs to be put in place to control the activities of these criminals in this area otherwise Nigeria economy may be brought down, particularly with trading on the country's stock exchange market going online. Without proper security methods in place, it is just like building a house without locks. Any person can gain access. The category and nature of cybercrime in Nigeria is endless. Cybercrime is a global phenomenal that is threatening the economy of nations. It is a major threat in India as it is in Nigeria. Punjab National Bank suffered a loss of close to Rs. 1. 39 chores when the computer recorders were manipulated to create false debits and credits. In bank of Baroda, Rs 2.5 lakh was misappropriated through the computerized creation of false bank accounts. In Mahanager Telephone Nigam Limited (MTNL) in Delhi, a junior telecom official was charged for reversing electronic telephone meter system thereby allowing some commercials export houses to make overseas calls without the charges being directed to their telephone numbers.

Understanding Cybercrime in Nigeria

The internet as an instrument to aid crime ranges from business espionage, to banking fraud, obtaining un-authorized and sabotaging data in computer networks of some key organizations. Prevention of cybercrime requires the co-operation of all the citizens and not necessarily the police alone who presently lack specialists in its investigating units to deal with cybercrime. The eradication of this crime is crucial in view of the devastating effect on the image of Nigeria and the attendant consequence on the economy.

Materials and Methods Used in Cybercrime

Technology has integrated nations and the world has become a global village. The economy of most nations in the world is accessible through the aid of electronic via the internet. Since the Electronic market is opened to everybody it also includes eavesdroppers and criminals. False pretence, finds a fertile ground in this situation. Some perpetrators of this crime usually referred to in Nigeria as "yahoo boys" are taking advantage of e-commerce system available on the internet to defraud unsuspected victims who are mostly foreigners thousands and sometimes millions of dollars. They fraudulently represent themselves as having particular goods to sell or that they are involved in a loan scheme project. They may even pose to have financial institution where money can be loaned out to prospective investors. In this regard, so many persons have become a duped. Merchants who take orders from merchandise on credit are also facing mounting losses from rip offs. Our investigation revealed that "yahoo boys" also take undue advantage of some people that are looking for spouse through the aid of Internet. These criminally minded individuals usually have discussion with their victims via the internet. These criminals pretend to be interested and loving. And before the victim realizes what is happening, the criminals would have succeeded in cajoling them to send some dollars to enable them to facilitate traveling documents. These criminals falsify document and tell all sort of lies to get money from their victims, when their victims begin to suspect foul play, they will immediately stop interacting with them and shift their target elsewhere. Cybercrime in Nigeria is difficult to prove as it lacks the traditional paper audit trail, which requires the knowledge of specialists in computer technology and internet protocols. Specific computer crimes are Spam, Fraud, Obscene or offensive content, Harassment, Drug trafficking, and Cyberterrorism.

Extant Laws to Combat Cybercrime in Nigeria- Presently, in Nigeria there is no specific law to combat cybercrime. The criminals are just operating freely without any specific law to checkmate their illicit activities. However, there are laws though not directly related to cybercrimes but in a way can to a limited extent be used to deal with this issue. These laws are: Economic and Financial Crimes Commission (Establishment) ACT 2004, Nigerian Criminal Code. The activities of the "Yahoo boys" are sabotage on the economy of the country. To this extend it constitute economic crimes which Economic and Financial Crimes Commission (Establishment) Act can deal with. Economic crime is defined as; "the non- violent criminal and illicit activity committed with the objectives of earning wealth illegally either individually or in a group or organized manner thereby violating existing legislation governing the economic activities of government and its administration to includes any form of fraud, narcotic drug trafficking, money laundering embezzlement, bribery, looting and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labour, oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and policy, open market abuse dumping of toxic wastes and prohibited goods e.t.c". The other available law is the Nigeria criminal code, which can also presently be used to prosecute these criminals. Most of the activities of these criminals bother on false pretences and cheating which sections 419 and 421 of the Nigerian Criminal Code prohibits respectively. Section 418 defines obtaining property by false pretence as follows; "Any representation made by words, writing, or conduct, of a matter of fact, either past or present, which representation of false in fact and which the other person making it knows to be false or does not believe to be true, is a false pretence".

Section 419, provides as follows; "Any person who by any pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years". "If the thing is of the value of one thousand naira or upward, he is liable to imprisonment for seven years". "It is immaterial that the thing is obtained by or its delivery is induced through the medium of contract induced by the false pretence. The offender cannot be arrested without warrant unless found committing the

offence." The definition of economic crime referred to above is all embracing. It means the jurisdiction of the Commission covers a wide range of criminal activities including fraud. Fraud, the noun variant of fraudulently, is

(i) an action or a conduct consisting in a knowing representation made with intention that the person receiving that misrepresentation should act on it

(ii) the misrepresentation resulting in the action or a conduct;

(iii) an action or a conduct in a representation made with the intention that the person receiving that misrepresentation should act on it and so on and so forth.

Despite the effort of the commission in this regard, it has been difficult to actually bring these boys to book in view of the complexity of the nature of the crime and investigation that needs to be carried out for proper prosecution of a culprit o this crime. Flowing from the provision of section 419, false pretence means; knowingly obtaining another person's property by means of a misrepresentation of facts with intends to defraud. Nigeria is a place where computer can be used to commit all sorts of crimes without prosecution, as there is no law on cybercrime. The Nigerian police simply lack Internet policing capability. Nigerian law enforcement agencies are basically technology illiterate, they lack computer forensics training and often result to conducting police raids on Internet service site mainly for the purpose of extortion. It is very common for the police to demand bribe from cybercafé operators that owns sites where suspicious activities are taking place and look the other way. There are so many reports on Nigeria cybercrime situations that well-meaning Nigerians are no longer comfortable with anymore. These reports are damaging the dignity of our country as a sovereign nation. They are humiliating and injuriously affecting our international image, our business, our mental – psychology and even our children. However, these reports points towards the fact that Nigeria is operating on a weakened technology platform and digitally illiterate environment that is in urgent need of expert solution.

Root Cause of Cyber insecurity in Nigeria

– Poor Promotion of recruitment, training, upgrade in technical skills and development of cyber security personnel in Nigeria. This root cause results in shortage of security agents with top notch skills to trail apprehend investigate prosecute and punish cyber criminals. The resultant effect of this creates a near safe haven for these cyber criminals to operate hence making the Nigerian cyberspace very insecure.

– Lack of proper feasibility by the government before implementing certain economic policies, for example the FOREX policy. Some of these policies render the Nigerian business terrain unfavourable for investors hence old investments pull out or cut down on staff, while there are no new investments coming up. This causes unemployment. High rate of unemployment and poverty now propel the youth to take to cybercrimes. Again, the Nigerian citizens often celebrate criminals and play sycophancy around them just to get miserly peanuts from them. A common scenario where Cyber Criminals who throw money around become mentors to these vulnerable and unemployed youth in the country hence promoting cybercrimes and rendering the Nigerian cyber space insecure.

– Sabotage by regulation and monitoring agencies render the energy sector unfunctional hence making the country unfavorable to investors, this leads to high rate of unemployment in Nigeria. economy before they are implemented. them with global best practices to avoid implementing economic policies that will trigger a negative ripple effect on the nation and scare investors and job creators away. Sabotage by the monitoring and regulation agencies render the energy sector unfunctional Overhaul the monitoring agencies to fish out and punish the saboteurs in the energy sector. Sabotage by the elite politicians and poor funding of security agencies lead to insecurity in Nigeria today. Proper funding of the law enforcement agencies to enable them do their job well and keep the nation Safe, hence attract investors.

– Sabotage by the elite politicians and poor funding of the security agencies cause insecurity which scares investors away leading to unemployment.

Proliferation of Cyber insecurity in Nigeria

In Nigeria, perpetrators of cyber-crimes engage in these activities because of the following 1. The huge financial benefits accruing from cyber-crimes. 2. Cyber-crimes attracted mild punishment as provided by law. 3. Cyber-crimes are always almost not properly investigated and prosecuted in Nigeria. 4. The cyber criminals have expert knowledge of how to manipulate and navigate through computer systems, networks and devices. 5. Hitherto to passage of the cyber-crime bill of 2015, the cyber criminals had a safe haven to operate as majority of their criminal activities were not considered criminal offences 6. The law enforcement agencies do not have the required expertise, technologies and techniques to thoroughly investigate and prosecute these cybercrimes.

Impacts of Cyber insecurity on the Nigeria State

Hassan et al. (2012) identified reduction in competitive edge of organizations, time wastage and slow financial growth, slow production time and increase in overhead cost, as well as defamation of the image of a nation as some effects of cybercrime. Other major effects include monetary losses and loss of privacy. Some of the effects of cybercrime are briefly explained below: (i) Reduction in Competitive Edge- An organization can lose its competitive advantage and suffer losses when a hacker steals

its confidential information and future plans and sells it to a competitor. The time spent by IT personnel on rectifying harmful incidents caused by computer criminals could have been used to earn profit for the organization.

(ii) Productivity Losses and Rising Cost- Cybercrime also reduces the productivity of an organization, as businesses take measures to prevent it by securing their networks. This is time consuming and also affects productivity. In addition, to control viruses and malware, organizations buy security software to reduce the chances of attacks. Computer crime therefore increases overhead cost and reduces profit margins. Other effects include the consumption of computer and network resources, and the cost in human time and attention of deleting unwanted messages.

(iii) Monetary Losses- The financial costs to economies and businesses from cyberattacks include the loss of intellectual property, financial fraud, and damage to reputation, lower productivity, and third-party liability. Opportunity cost (lost sales, lower productivity, etc.) make up a proportion of the reported cost of cyber-attacks and viruses. However, opportunity costs do not translate directly into costs to the national economy. Businesses face greater damage from financial fraud and intellectual property theft over the Internet. Thus, where cybercrime is rife (especially relating to businesses and financial institutions) there are bound to be untold financial consequences. A research report by Ponemon Institute (2016) shows that, cybercrime cost in six countries (U.S.A, Japan, Germany, U.K, Brazil and Australia) in 2016 ranged from USD$4.3 million to USD$17.3 million annually. The study used a sample of 237 companies in the six countries.

(iv)Destroys Country's Image- One key negative effect of cybercrime is that it tarnishes a country's image. Once a country is labeled as a harbor for cybercrime activities, potential investors are cautious in investing in such countries. This has some dire implications for the nation's macroeconomic stability.

(v) Retards Financial Inclusion- proliferation of cybercrime in a particular country discourages financial inclusion, due to the fear of being a victim of cyber-attack.

Unabated Cyber Terrorism and Human Security in Nigeria

The advent of cyber as a weapon of warfare is rapidly gaining momentum not only in Nigeria but globally. Terrorists now employ it to monitor individuals, governments and security networks as well as to attack institutional or governmental facilities (Ntamu, 2014; Onuoha, 2011; Yar, 2006). Beyond the traditional and conventional style of terrorist activism, the violent rise of the jihadist group Boko Haram in Nigeria's Northeast region has now dominated policy debates among academics and policymakers not only in Africa but beyond. Boko Haram membership which prefers to be called by the Arabic name Jama'atu Ahlis Sunna Lidda'awati wal-Jihad, meaning "People of the Sunnah (the practice and examples of the Prophet Muhammad's life) for Preaching and Jihad Group" is believed to be founded by Mohammed Yusuf in the town of Maiduguri, Northeast Nigeria in 2002. It has since 2015 transformed to become one of the deadliest terrorist groups globally (Global Terrorism Index, 2016). Boko Haram which is a combination of two Hausa words boko meaning Western education/civilization and haram meaning sin or forbidden. Thus, combined means western civilization is forbidden. It is also believed that the membership of over 500,000 people who were generally disgruntled with the situation in Nigeria especially the configuration of the political and economic structure was taxed one Naira daily to sustain their ideology (Adibe, 2013).

The Nigerian government had claimed decimating the Boko Haram sect, but the reality is that warfare of the 21st century has gone from hardware to software. The group has strategized to using not only physical weapons of warfare but unconventional tactics to cramp the government. Beyond throwing bombs, taking hostages and crossing borders they now target critical national infrastructure by attacking the cyber security of Nigeria. Their adoption of cyber technology for technology integrated intelligence through the use of ICT devices such as computer, internet, mobile phone, Close Circuit Television, surveillance camera, social network, biometric surveillance, data mining, satellite imagery, IP devices and other technologically driven weapons is believed to have aided their collaborative efforts with others like Al Shaba of Sudan, ISIS and al Qaeda to unleash terror on citizens not only in northern Nigeria but also to the neighboring Chad, Niger and Cameroon (Adam, Osah, & Alao, 2019; Jacob & Akpan, 2015; Obayuwana, 2011; Osho, Adesuyi, & Shafi'l, 2013). This is what Aladenusi (2015) calls 'cyberharam'.

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 propagations, 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 to curtail them. This explains why Arimatéia da Cruz (2013) noted that apart from using internet to launch cyber-attacks against countries, terrorists possess the capacity to engage in "hacktivism," which is described as strategy of merging hacking and activism. The implication is that the seven dimensions of human security namely economic, food, health, environmental, personal, community and political as established by the United Nations Development Programme (UNDP) in 1994 might be difficult to attain as a result of terrorism by 2030 being the set target of the Sustainable Development Goals (SDGs) if nothing urgent is done to reverse the trend.

Cyber information sharing: what is it and why does it matter?

No single organization or country has visibility over the entire problem space, making collaboration and information sharing essential. Knowledge is power. Intelligence, carefully curated from the collection, evaluation and assessment of data from many sources is fundamental to understanding the complex and dynamic threats that exist in the information age. Once only the preserve of government departments and military agencies, intelligence now helps businesses and global institutions make

better, data-driven decisions. It gives them the edge in formulating new plans and strategies to manage risk, and to perform efficiently and effectively. Cybersecurity is defined by its multi-stakeholder ecosystem and needs to be seen from a holistic viewpoint. All participants in that ecosystem need to be able to participate in building the systemic resilience of the collective infrastructure on which those stakeholders rely.

Seven key challenges that Nigeria and the global security community needs to address

1. Gaps in jurisdictions and cross-sector collaboration Even where there is relative maturity in sectors for information sharing, trust and barriers to collaboration remain between regions. In Africa, just eight countries have a national strategy on cybersecurity and only 13 have a Government-Computer Emergency Response Team, which typically act as vehicles for establishing national information sharing programmes.

2. Skills and capabilities -The cybersecurity skills gap is well documented. In the 2020 UK Government Cybersecurity skills report, threat intelligence was listed as one of the most sought-after technical skills. Nearly one-fifth of all businesses that responded stated they had a skills gap associated with threat intelligence, which was the fourth-highest technical skill gap listed after security architecture, forensics and penetration testing. This assertion is very true in Nigeria's context.

3. Trust and privacy- There is a lack of trust between key players at operational and governmental levels, which needs to be developed to facilitate information sharing. Geopolitical drivers and fragmentation in international co-operation can affect public-sector enthusiasm for data exchange programmes. The private sector is often reluctant to share information with governments for fear of regulatory impact, to avoid complicity in any privacy and rights violations and because they often see no benefit to doing so. Cross-sector information sharing is further hampered by fears about giving competitors an advantage, as well as concerns about sharing sensitive internal data. Free cross-border information sharing is additionally complicated by the possible threats to human rights protections when information is shared with states that have a weak rule of law and or a history of systemically violating human rights.

4. Legislation, policy and data fragmentation There is a current lack of alignment and harmonization across jurisdictions – and in many cases conflicting regulations in relation to the sharing of cyber information – especially with regard to concerns over the disclosure of what could be considered as sensitive proprietary information by an organization. More dramatically the trend towards data localization – where governments mandate that data on their citizens or residents can only be stored within their country, and-or meet local privacy and security mandates before being transferred externally, can frustrate, or outright forbid, the fluid sharing of certain information.

5. Operational costs -To be able to effectively receive, analyse and action cyber intelligence into the full defensive posture, the institutions of Nigerian state require investment in the right technology, staff and governance. For decision-makers and industry leaders looking to reap the rewards of participating in an information-sharing ecosystem, estimating the costs and targets for tangible investments is often difficult due to the array of options and lack of agreed standards from which to measure the benefits of such investment. Even where information-sharing programmes are available, participation costs act as a barrier. Security budgets in countries, particularly those in developing economies, are focused only on the most immediate concerns and seldom a more holistic, mature strategy.

6. Lack of clear incentives Cybersecurity information sharing lacks traditional, positive incentives (the tangible short-term protective benefits, liability protections, insurance incentives) and negative incentives (compliance requirements, regulatory pressures). Organizations are often concerned about reputational damage or legal exposure for revealing the particular attacks they experienced, especially if the attacks were neither avoided nor defended as well as the firm would have wished. Without tangible short-term incentives in place organizations operating within the Nigerian border are not likely to prioritize cybersecurity information sharing.

7. Operational, interoperability and technology barriers Multiple standards, frameworks and technologies exist in relation to cyber information sharing presenting a further barrier to widescale adoption. Technical standards authorities, national bodies and certain sector groups implement specific solutions attuned to their environment, but more work is needed to be able to provide interoperability throughout the ecosystem to ensure cyber information-sharing practices can be harmonized. The lack of harmonization not only makes interoperability difficult, but it forces privacy and other rights-based considerations to be re-evaluated for each new standard and/or framework creating additional unnecessary hurdles. While there are no-cost and open-source technologies such as MISP, The Hive, Cortex and IntelMQ, there are still significant technical resources required to implement technology to create and/or participate in cybersecurity information-sharing communities. This can reduce the overheads of producing information and/or refining others' information into actionable intelligence or allow easy integration between threat information sharing feeds and the range of security/investigation tools used by defenders.

Cyberterrorism and the Protection of Critical Information Infrastructure in Nigeria: A Legal Assessment

The well-being of any nation depends upon secure and resilient critical infrastructure. Government business can be brought to a halt if critical information infrastructures are attacked. Similarly, many private businesses may also grind to a halt if critical information infrastructures are attacked. Critical infrastructure refers to the various systems, networks, facilities and services upon which the daily life of a nation depends. One of such infrastructures is the power network that provides the nation with electricity. A major attack on a nation's power grid would shut down any country. The advent of cyber as a weapon of warfare is rapidly gaining momentum the world over and Nigeria is not immune to such threats. In 2012, it was reported that there was

about 60 percent increase in the attacks on Nigerian Government websites. This paper examines the concept of cyber-terrorism and the possibility of terrorist organizations like the Boko Haram sect using the cyber to perpetrate terrorist acts in Nigeria. The paper argues that the Cybercrimes (Prohibition, prevention) Act 2015, in its current state cannot adequately address the issue of cyber-terrorism and the protection of critical national infrastructure in Nigeria. The law does not provide for a single enforcement institution and as such the enforcement framework is chaotic. This paper suggest an amendment to the Act and to include the creation of a cyber-attack prevention agency that will be saddled with enforcement of the Act and developing the technical capacity of local technocrats to be able to manage the cyber security risks to Government and private sector critical information infrastructure.

Cyber-terrorism in Nigeria: Is the threat real? Terrorist cells in over 60 countries have resorted to the use of cyberspace to recruit their members, spread propaganda, raise money, train more terrorist and conspire to intimidate and coerce government and innocent citizens in furtherance of their political and religious objectives. Social media platforms are now avenues for the terrorists' use for coordination of their illicit actions and spread of messages. Terrorists use of the internet, especially social media to propagate messages involve a mix of social media savvy, tactical use of technology, and the nature of the internet itself as an isolating yet supportive force for some people, enough to drive some to become terrorists themselves. They mostly use targeted social media campaigns by way of hash-tags to gain attention and support. The number of sites that terrorists have been using is extensive: Twitter, facebook, instagram, you tube and flickr. In August 1999, it was reported that almost every terrorist group had established their individual websites, along with a mishmash of freedom fighters, crusaders, propagandists and mercenaries. The internet serves as an appropriate haven for them to engage in conferences and debate on their premeditated objectives through the use of web forums, emails, and chat. The internet has the ability to connect not only members of same terrorist organizations but also members of different groups. Al Qaeda members (which are at present the most notorious terrorist group) have mastered the art of using the cyberspace to advance their own goals. Osama Bin laden, Isis and Boko Haram have reportedly posted web pages on the internet to gain support and followers, and also in furtherance of the spreading of their messages. The headquarters of Osama Bin Ladin in Afghanistan was reported to have been equipped with computers and communications equipment as at 1996-7. In Nigeria today, the greatest and predominant security challenge that the country is facing is terrorism. The jarna'atu Ahlis Sunna Ladda Watin Wal-Jihad, a religious based Islamic fundamentalist group popularly known as Boko Haram is the harbinger of terrorism in Nigeria today. The sect which is predominantly based in the North Eastern part of the country has an ideology that is averse to Western education and anything it represents. The sect also seeks an enthronement of Islamic (Sharia) government in the whole of Northern Nigeria. Adherents of Boko Haram attack government institutions, such as the police and military through armed attacks or suicide bombing. The sect was founded by Mohammed Yusuf in 2001. Because of its claim of wanting to establish Sharia law in Nigeria, it is sometimes referred to as Yusufiya group. The unfortunate association of Islamic religion with terrorism has been as ancient as 622/623 AD when the religion was found. Islam started by the sword through conquests made by Prophet Mohammed culminating in the Hijiriah from Medina to Mecca in 623 A.D. The Boko Haram sects in Nigeria operates as a faceless group of militants who carryout coordinated surprise attacks on defenceless citizens by striking them at churches, markets, offices, relaxation sports etc. Usually a suicide bomber on a motorcycle, can hit its target and dies with the victims. But in June 2011, there was a significant shift in Boko Haram's targets, tactics and geographic reach. The use of a suicide VBIED (vehicle-borne improvised explosive device) on the Abuja police barrack marked the first time on record a suicide attack was carried out in Nigeria.Boko Haram has international links with other terrorist groups such as the Al-Qaeda in the Magherb (AQIM), Al-Shabab in Somalia. Boko Haram's evolving tactics and targeting may be the result of ties between AQIM in North Africa and Al-Shabaab in Somalia. Such cross-pollination of weapons, tactics, and bomb-making expertise had increased the capabilities of the terrorist group. On June 14, 2011, AQIM leader Abu Masab Ab al-wadoud, also known as Abdelmalik Droukdel, told Al Jazeera that his group would provide Boko Haram with weapons, support and training. In September 2011, threats made by Boko Haram to bomb Lagos Airport prompted security officials to search all vehicles approaching the airport, causing major disruptions. Even more indicative of the growing sophistication and threat potential of Boko Haram is the groups increased use of the internet forums. According to a September 28, 2011 report published by the SITE intelligence group, Boko Haram had developed an increased online presence that seems to have contributed to the rapid increase in their strength. The sect has been getting tremendous support from these groups. It is becoming increasingly clear that as technology advances, the tools used by the sects in their destructive and terrorist activities will no longer be guns, and bombs but other weapons of mass destruction and attacks on critical infrastructure using the computer.

Solution

Nigeria's Approaches in Combating the Menace of Cybercrime/Cybersecurity

Azazi (2011) set up a Committee on cybersecurity Legislation to access the Nigeria cyberspace. In the report submitted to the office of the National Security Adviser (NSA), the committee revealed the followings:

1. Nigeria lacks the structures to handle any cyber-attack emergency, with the increase in bomb attacks and growing threat of attacks through computer networks.

2. There is no comprehensive assessment of the preparedness of the country in the event of cyber-attacks.

3. There is no focal point for coordinating cybersecurity in Nigeria.

4. There are no structures to handle any emergency cases of cyber-attacks.

5. The current legal framework is grossly inadequate for cybersecurity in Nigeria and does not support a coordinated approach to developing a cybersecurity strategy. The committee further revealed that, the challenges in developing a cybersecurity framework to include;

lack of awareness and jurisdiction overlaps among existing law enforcement agencies.

Others are the absence of certification of critical national information infrastructure and the absence of systematic capacity and capability building for law enforcement agencies.

The committee recommended that the office of the National Security Adviser (NSA) should initiate the amendment of the National Security Agencies Act, Cap N74 LFN 2004 to create the Directorate of Cybersecurity; liaise with the Office of the Attorney General of the Federation and Minister of Justice and work with legislators to ensure the passage of the harmonised cybersecurity Bill. Sorunke (2011) maintained that Nigeria at the cyberspace is under threats, with much vulnerability, many loopholes in our system and with issues bothering on our payment networks. He warned that, if urgent measures were not taken by businesses and government organisations deploying web-based platforms for their operations and with the increasing rate of cyber insecurity in Nigeria; companies might soon be faced with high incidence of hacking, leading to loss of data critical to a business life and revenue. He maintained that, the high level of insecurity in the Nigeria's cyberspace might affect the cashless economy objective of the Central Bank of Nigeria. He noted that the wanton defacing of some government websites such as the Niger Delta Development Corporation (NDDC), Power Holding Company of Nigeria (PHCN), etc. by a group of hackers known as NaijaHacktivists; in practical terms inform how vulnerable most Nigerian organisations were in the cyberspace. From the above, it is obvious that the Nigeria's cyberspace is porous and has no form of legal protection to regulate activities in Nigeria's cyberspace.

The Cybercrimes (Prohibition, Prevention) Act 2015 In the wake of advancement of technology, several conventional crimes which were hitherto only committed against per sons physically or in direct contact with the assailant or criminal has now shifted to the internet where such offences can be committed over the internet with the use of the computers and without the victim even getting to know or meet the offender. This ugly development amongst other factors necessitated the enactment of the cybercrimes Act in Nigeria. The cybercrime Act was signed into law on May 15, 2015. The Act provides an effective, unified and comprehensive, legal, regulatory and institutional framework for the prohibitions, prevention, selection, prosecution and punishment of cybercrimes in Nigeria. The Act is made up of 59 sections, 8 parts and 2 schedules. The first schedule which is section 42(1) lists the members of the cybercrime Advisory council. The second schedule which is section 44(2) (a) provide for businesses to be levied for the purpose of the cybersecurity fund. The Act covers broad spectrum of list of cybercrime offences punishable with penalties and fines in part III., which includes offences against critical national information infrastructure, unlawful access to computers, system interference, interception of electronic messages, e-mails, electronic money transfer, Tampering with critical infrastructure, willful misdirection of electronic messages, unlawful interception, computer related forgery, computer related fraud, theft of electronic devices, unauthorized modification of computer systems, network data and system interference, cyber-terrorism, fraudulent issuance of instructions, identify theft and impersonation, child pornography and related offences, cyberstalking, cybersquatting, Racists and xenophobic offences, importation and fabrication of e-tools, breach of confidence by service providers, manipulations of ATM/POS terminals, phishing, spamming, spreading of computer virus, dealing in card of another, purchase or sale of card of another, use of fraudulent device or attached e-mails and websites. Part II of the Act specifically provides for the protection of Critical National Information Infrastructure, while section 18(1) of Part III provides for the offence of cyber-terrorism. The section provides as follows: A person who accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and is liable to life imprisonment. The Act seems elaborate, but it may not be able to effectively address the issue of cyber-terrorism and the protection of critical national information infrastructure owing to several pitfalls in the Act. First, the law does not provide for a single enforcement institution. Section 41 (1) vest the enforcement of the Act on the National Security Adviser while section 41(2) and section 52(1) and (3) vest the powers of enforcement of the Act on the Attorney-General of the Federation. This is capable of creating conflict in the enforcement of the Act. Secondly, Nigeria over the years is fond of appointing retired military personnel as National Security Adviser. Sadly enough, most of these retired military officers so appointed are actually novice in cyber security which is quite different from conventional security. The Act did not spelt-out what should be the qualification of the National Security Adviser. Moreover, the duties assigned to the office of the National Security Adviser by virtue of section 41(1) of the Act are too technical to be left in the hands of a National Security Adviser who may not have any knowledge of Cyber-Security. The duties require someone with adequate knowledge of cyber and computer related issues.

The Federal Government of Nigeria modalities for implementation of the new National Cybersecurity Policy and Strategy (NCPS) 2021.

The Policy and Strategy is said to be a framework that aims to strengthen cybersecurity governance and coordination and foster a trusted cyber environment that optimizes Nigeria's cybersecurity readiness and coordination capacities towards addressing the nation's cyber risk exposure. This new policy is a review of the 2014 edition of the same, designed to realign the nation's cybersecurity efforts to effectively confront the dynamic and emergent nature of threats in the country's cyberspace. With over 104 million active internet users coupled with the local innovations that have made Nigeria one of the leading digitally connected countries on the continent and the prevailing challenges that come with cyber penetration, this review has become very important. Here are few things you should know about this policy: To effectively carve this policy, these seven have been identified as the major cyber threats that the country is facing- Cyber-terrorism, Cybercrime, Online

child abuse, Election interference, Online gender exploitation and Pandemic induced cyber threats.

What are Nigeria's cyber vulnerabilities and strengths? To ensure risk assessment, the National Cybersecurity Coordination Centre (NCCC) identified some of the areas that are the weaknesses of the nation's cyberinfrastructure. The Centre admits that the country relies largely on foreign ICT solutions, therefore, citing research and development and human resource capacity as some of the weaknesses. Aside from these, low awareness about cybersecurity is also a limitation as opposed to the fast-growing pace of cyber threats. However, the Centre stated that the local private sector is well informed and proactive in the global cyber security market. Thereby, enabling multi-stake-holder's engagements in the sector.

What's the Policy Direction-The policy is hinged on protecting national security, strengthening economic development and fighting corruption. This is because the security and wellbeing of citizens are equally important in the cyber and physical domains, and cybersecurity is also a critical enabler in economic progression and other national priorities. Hence the need for the 12 pillars will create the foundation of delivery and possible collaboration between stakeholders. The pillars are;(a).Enhancing cyber defence capability, (b).Enhancing international cooperation, (c).Promoting a thriving digital economy,(d).Assurance monitoring and evaluation, (e).Strengthening the legal and regulatory framework, (f).Enhancing cyber security incident management, (g).Strengthen cybersecurity governance and coordination, (h).Fostering protection of critical and national information infrastructure.

Critical Sectors - In fostering the protection of critical national information infrastructure, the policy identifies the following as 'critical sectors'; (a).Water, (b).Health, (c).Education, (d).Transport, (e).Public Administration, (f).Defence and Security, (g).Banking, Finance and Insurance, (h).Safety and Emergency Services, (i).Information, Communication, Science and Technology, amongst others. Aside from this, the policy explored the legal and regulatory framework of cybersecurity with keen attention to internet safety and child online protection. Also, the establishment of the National Digital Forensics Laboratory under the NCCC is mentioned as one of the strategies to be implemented to enable the war against various cyber threats.

Practical Challenges to Prosecuting Perpetrators of Cyber-terrorism. The Prosecution of Perpetrators of Cyber-terrorism is not without challenges. Some of the identified challenges affecting the effective prosecution of cyber-terrorism offenders are: Jurisdictional issues, Evidential issues and Extradition. These factors militating against the effective prosecution of perpetrators of cyber-terrorism are treated below:

a) Jurisdictional Issues While the world we live in is physically demarcated in boundaries and territories, the world of cyberspace does not recognize any physical or political barriers or national frontiers. In plain words, cyber world is transnational, a global medium devoid of any territorial divisions. The unbounded nature of the internet has challenged the basis for the traditional notions of jurisdiction which are predicated on real space demarcation. Because, a page on a worldwide web can reach web surfers in every state in the nation and perhaps every nation of the earth, there arises the issue of where exactly a person who has a cause of action, based upon web transaction may sue. In order for any court of law to try and punish a cyber-terrorist, such a court must be cloth with the legal authority to do so. The legal authority that empowers a court to so Act is referred to as jurisdiction. In simple words, jurisdiction is the power of a court to hear and determine a case. Jurisdiction is the legal capacity of a court to hear and determine judicial proceedings. It is the power to adjudicate concerning the subject matter of the controversy. A court of Law can only exercise judicial powers when it has jurisdiction. Without jurisdiction, a court's judgement will be ineffective and impotent. The determination of Jurisdiction in respect of cyber-terrorism offences could be cumbersome and mostly difficult for the courts to determine. The virtual world seems to be a borderless Journey to the wonderland. This has continued to cause confusion and misapplication of legal principles for the enforcement of cyber-terrorism adjectival laws. For instance, in the case of **R. v. Governor of Brixton Prison and Anor, Ex-parte** Levin, Where one of the issues for determination was whether the locus in quo of the offence was in St. Petersburg, Russia, where the computer instructions were sent, or in victim's computers in Parsippany, New Jersey in United States. The Court held that given the virtually instantaneous nature of electronic transaction, it was 'artificial' to regard the offence as having occurred in one place or the other. Could it then have been right to say that cyber-terrorism offences lack any locus delicti; or could the offences be said to have multiple locus delicti? Since cyber-terrorism offences are usually cross-border offences involving multiple Jurisdictions; which state could rightly assume Jurisdiction? These Questions have necessitated the need for various states to include provisions conferring the national courts with extra territorial jurisdiction.

b) Evidential issues Criminal Prosecutions can succeed or fail based upon the evidence presented. Loss or contamination of evidence in the cause of cyber-terrorism investigation is a very common and also an obvious problem which may affect the veracity to be attached to the piece of evidence, or even jeopardize the entire Criminal Proceedings. The collection of data outside the physical, territorial boundaries have also proven to be one of the most important issues that could also paralyse cyber-terrorism investigations and any consequential prosecutions. Prosecutors of cyber-terrorist will often have problems getting access to relevant documents. Where documents are available, the courts will face special challenges in verifying whether they are authentic. Also, obtaining witness testimony is quite difficult. The process of compelling witnesses who can give direct testimony is quite cumbersome sometimes owing to the distance involved.

c) Extradition The prosecution of cyber-terrorists sometimes involves one state requesting the extradition of a suspect from another state. Extradition laws generally provides for a complex legal process which can take months if not years to reach its conclusion. Also, many states usually refuse the extradition of their own nationals who have taken refuge in their territory,

although as between states who observe absolute reciprocity of treatment in this regard, request for surrender are sometimes acceded to. International Law concedes that the grant of and procedure as to extradition are most properly left to municipal law, and does not, for instance, preclude states from legislating so as to refuse the surrender by them of fugitives, if it appears that the request for extradition had been made in order to prosecute the fugitive on account of race, religion, or political opinions or if the fugitive may be prejudiced thereby upon eventual trial by the courts of the requesting state.

Recommendations

Cybersecurity and cybercrime have emerged as a very concrete threat in Nigeria and the existing legislations in Nigeria are inadequate to address its threats. On this note, the following are suggested and recommended

1. There should be continuous revision and remodeling of the newly signed Nigeria National Cybersecurity Policy and Strategy (NCPS) 2021. Waiting for every 5 years before this is done will make Nigeria not to be abreast with the everyday dynamics and happenings in the cyberspace.

2. There is a need to protect all critical information infrastructures and secure computer systems and networks within Nigeria's cyberspace.

3. The establishment of national Computer Emergency Response Team (CERT) centre for the monitoring, detention and analysis of all activities within the Nigeria cyberspace and the globe at large.

4. The establishment of fully functional national digital forensic laboratory in the Office of the National Security Adviser (ONSA). This is to avail all law enforcement and security agencies a platform for detailed investigation of cybercrimes in Nigeria.

5. There is a need for a 24/7 emergence response website where victims can report all cases of internet fraud and cybercrime at large and know that, it will be given attention swiftly and in a transparent manner.

6. The government should determine their training needs in the area of cybercrime and explore bilateral, regional and multilateral cooperation mechanisms to meet those needs.

7. The government should heighten awareness of the dangers of cybercrime amongst the general public, including users in the education system, the law and security enforcement agencies, and the justice system on the need to prevent and combat cybercrime.

8. The implementation of General Data Protection Regulation (GDPR) that will not have any major impact on the information-sharing landscape, which may result in making some organizations fearful of breaching it. While there has been progress in jurisdictions such as the United States in providing greater legal clarity for cyber information sharing, more work is needed to provide the level of assurance required. Information sharing between national and supranational authorities to drive collective investigations should not be complicated thereby ensuring robust disclosure and the evidential proceedings required to ensure appropriate due process and public oversight are in place.

Conclusion

Until cyber criminals in Nigeria are convinced that no matter how crafty they are or the expertise they possess, that their crimes can be forensically investigated and that they will possibly face long jail terms or huge fines, Nigerian cyber security will not be assured. It has been seen that most cyber criminals have a loose network wherein they collaborate and cooperate with one another. Unlike the real world, these criminals do not fight one another for supremacy or control. Instead they work together to improve their skills and even help out each other with new opportunities. Hence, the usual methods of fighting crime cannot be used against cyber criminals. While law enforcement agencies are trying to keep pace with cyber criminals, it is proving to be a Herculean task. This is primarily because the methods used by cyber criminals and technology keeps changing too quickly for law enforcement agencies to be effective. That is why commercial institutions and government organizations need to look at other methods of safeguarding themselves. One of the best ways to avoid being a victim of cyber-crimes and protecting your sensitive information is by making use of impenetrable security that uses a unified system of software and hardware to authenticate any information that is sent or accessed over the Internet. Secondly a formidable framework should be put in place to track, detect, investigate and prosecute cyber-crimes, hence making it unsafe for cyber criminals to thrive. This is can be achieved if the computer forensics investigation profession and its practice is promoted in Nigeria.

Reference:

1. https://ndic.gov.ng/wp-content/uploads/2020/08/NDIC-Quarterly-Vol-34-No-12-2019-Article-The-Impact-Of-Cybercrime-On-The-Nigerian-Economy-And-Banking-System.pdf
2. https://www.ajol.info/index.php/stech/article/view/161143
3. https://www.researchgate.net/profile/John-Odumesi/publication/263967391_Combating_the_Menace_of_Cybercrime/links/00b4953c7613e08fbd000000/Combating-the-Menace-of-Cybercrime.pdf
4. https://pdfs.semanticscholar.org/a4f4/5ad4647a1fe0094317393997f353cc8a18e3.pdf
5. https://www.ajol.info/index.php/stech/article/view/154713
6. http://ctc.gov.ng/wp-content/uploads/2021/02/NATIONAL-CYBERSECURITY-POLICY-AND-STRATEGY-2021_E-COPY_24223825.pdf

Appendix

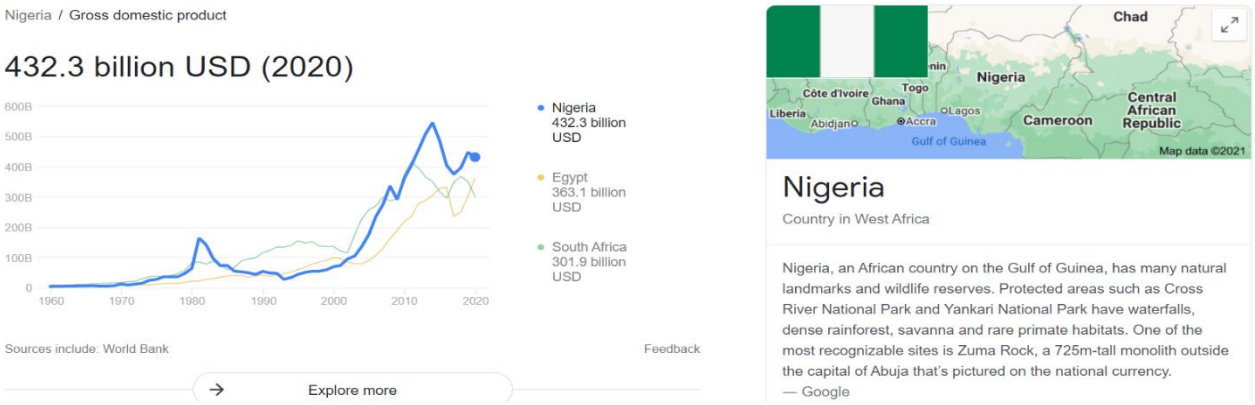

Fig 1

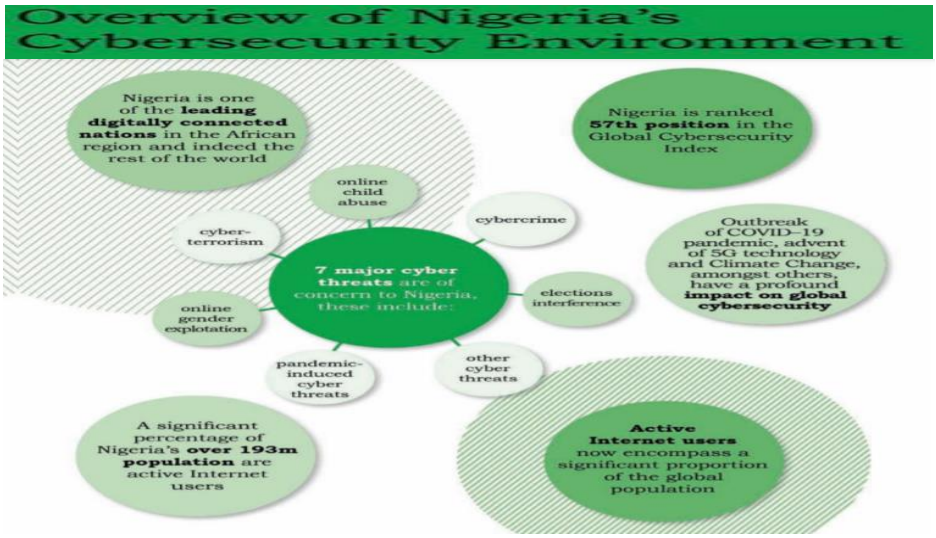

Fig 2

Fig 3