ADDRESSING INSECURITY ISSUES IN NIGERIA: CHALLENGES AND PROSPECTS OF CYBER-SECURITY

Bolarinwa. A. HARRISON
Department of Philosophy,
Osun State University
Email: harrisonayomide@gmail.com

Abstract
Insecurity has become a bane in the growth and development of Nigeria. Among the current security issues are kidnapping, terrorism, banditry, Niger-Delta militancy, insurgent groups and the Fulani herders/farmer clashes. However, one aspect of security often under-emphasised is the area of cyber-security. Among a large array of security challenges and problems is the issue of cyber-crimes, security and protection. Cyber security has risen to become a national concern due to the growing influence and advancement of technology; considering that a large amount of data and information continues to be stored in cyberspace and people are becoming more susceptible to cyber-attacks such as cyber-terrorism and hacking. The paper will be concentrating on the appraisal of the challenges and importantly the prospects of cyber-security and technology not only for curbing cyber-crimes and insecurity but ameliorating the growing list of internal insecurity in Nigeria. The paper argues further that investment in cyber software, design, policies, cyber-security training and creating legal frameworks will aid the fight against insecurity and promote the agenda of nation-building. The paper underscores the importance and purpose of cyber security in the modern internet era and how it can be used alongside the various physical security systems and law enforcement agencies for effective protection to ensure the security of lives and properties.

Keywords; Cyber-security, cyber-crime, security, development, nation-building

Introduction
It is a fact that the world has gradually become a global village and the question of world peace is now a matter of global concern as it affects people around the world. The problem of security in the cyber sphere is also a growing global issue. Nigeria as a member of this global village is not excluded from these security challenges. Nigeria is currently experiencing an unprecedented level of cyber-attacks both in information security, network security, data hacking, scamming and cyber warfare. In recent times, Nigeria has become a target of the prevailing series of cyber-crimes due to the availability of data from individuals, corporations and the government in cyberspace with a heavy reliance of the public on computer technologies, the internet and connectivity. More than ever, cyber security requires pertinent attention attributed to the continuous expansion and increasing use of digital and computer technologies. Cyber security is not only essential to large corporations

or corporate bodies or businesses but citizens as well as the general public. The perpetrators of cyber-attacks have no specific or intended target as anyone can be singled out and made a victim and everyone is at risk of cyber-attacks which exploit our computer's vulnerabilities from the use of our mobile phones to investment in banks, hospital appointments, and even the government database.

While the government remains actively engaged in ensuring protection and addressing other internal security issues within the nation, cyber-attacks such as cyber-terrorism, hacktivism, ransomware, among others, continue to rapidly increase and pose a significant threat to life and properties of citizens. Cyber-crimes are real threats that know no border, race, or background. They are virtual yet with physical implications for victims around the globe.

Security implies a guarantee of safety and protection of both lives and properties, hence considering that virtually all areas of our survival, i.e., food, health, travels, business, etc., rely on the use of digital tools, computer technologies and the internet, it is a given that cyber security should indeed be a source of concern and action for the government as well. In light of this, this paper examines the prospect of cyber-security in addressing the growing rate of insecurity in the cyberspace and recommends possible solutions to its challenges. The paper argues further that adequate education and training on cyber security alongside funding and investments in cyber tools and architecture can help minimise cyber risks, aid the agenda of nation building and development and also help ameliorate the straining effects of internal insecurity and challenges in the country.

An understanding of Cyber-spaceAccording to the Computer Security Resource Centre, cyberspace is defined as a domain within the information environment consisting of the interdependent network of information systems infrastructures including the internet, telecommunications network, computer systems and embedded processors and controllers (CSRC NIST, 2022). Cyberspace is a boundless space of unlimited data and information through interconnected networks also referred to as the internet.. Cyberspace describes a supposed virtual space that is created by interconnected computers and networks on the internet. It is an electronic space where people communicate. The cyberspace is regulated by a set of architecture—policies and designs known as cyber security architecture. Cyber security architecture is responsible for maintaining security and protection against threats or breaches. It detects future threats and provides a way of support for an organisation's system. It is the organisation's foundational defence that secures the information technology environment.

Cyber-Security Examined

Over the years, humans have witnessed a vast development in business, education, tourism, health technology and modern economy, etc. With the experience of the Covid-19 pandemic, the world has diverted into cyber world. Businesses migrated

to online platforms for sustainability and catering to a wider audience, schools began virtual training and lessons, and appointments that required walk-ins were mandated to online transactions and correspondence, leading to the development of internet applications that would enable stronger communications and smooth accessibility to cyber activities. The advancement of technology and its use has contributed immensely to various modern developments we currently enjoy. However, despite its merits and technological advancements, the internet has become a source of concern and unrest among individuals, businesses and the government. The use of technology, artificial intelligent agents and the human factor is largely responsible for the outbreak and alarming rate of cyber-crimes. Cyber-crimes are committed against unsuspecting users in cyberspace by unethical end-users, thereby threatening security and causing harm to other users and this has led to a high level of unprecedented threats and insecurity. Insecurity refers to a lack of protection and freedom from danger, physically, economically and socially. On the other hand, security is freedom from harm. Nevertheless, security is not the absence of threat; it implies a state of stability and continuity in the affairs of the state. It is a sense of peace and a guarantee of safety, to overcome the challenges that may threaten the expected conditions of safety. In recent times, there has been a dearth of data protection in ensuring the public's security as it pertains to their data and properties in the cloud and cyber-space. Data are individual facts, statistics and information about a person that has been translated for transmitting or processing on a computer or database (Vaughan, 2021). The majority of data and information are stored on the cloud; the cloud refers to a virtue storage space where files are stored for unlimited time and accessible to end-users.

According to Gaser (1988), cyber security is the protection or guarding of computer systems against theft or harm to the hardware, software or information, as well as from interruption or misleading and incorrect commands of the services they offer. Cyber security is the application of technologies, processes and controls to protect systems, networks, programmes, devices and data from cyber-attacks (REF). Cyber security includes the body of rules put in place for the protection of cyberspace (www.itgovernance.co.uk/what-is-cybersecurity). Cyber-attack refers to a series of organised crimes attacking both cyberspace and cyber security. Cyber security aims to minimise cyber attacks and protect individuals against unauthorised exploitation on the internet. According to the Australian Cyber Security Centre, there are four main principles of cyber security which are;

i. To govern and manage: identify and manage risks
ii. Protect: implementing security controls to reduce security risk
iii. Detect: detecting and understanding cyber security events.
iv. Respond and Recover: responding to and recovering from cyber security incidents.

As pointed out, cyber security is of great importance with the advent of smart devices such as smartwatches, smart TVs, mobile phones, etc. it is, therefore,

imperative to guard against damage that may occur due to the misuse and misconduct of certain end-users in cyberspace. The purpose of cyber security, therefore, is to maintain and sustain the safety, protection, confidentiality and integrity of data, information and network systems in cyberspace.

It is our belief that cyber security is a sub-part of national security and needs the intervention of the government to supervise internet activities and electronic communications, in curtailing security risks both in the cyberspace and the nation in general.

Types of Cyber-crimes include;
Ransomware: This refers to malware designed to deny individuals or user access to files by encrypting them and demanding payment. In most cases, network systems are infected with viruses or software intended to steal their personal information or files in exchange for a ransom. Malicious Software (Malware): Malware refers to software that has been intentionally designed to damage or gain control of a computer system or network such as viruses, worms or spyware.
Phishing: This is used to describe fraudulent and tricky messages sent to end-user for them to divulge personal information such as credit card details, and banking identity, and it can be done through emails, spam messages and scam links such as "you've won a lottery", "click here to participate in our survey and win $1,000", etc.

Cyber stalking, harassment and bullying: These have led to the loss of lives which in most cases are suicidal. According to Michigan Tech, cyber stalking pertains to unsolicited or unconsented conduct such as constant mailing or threatening messages. Stalking, on the other hand, refers to the use of the Internet to stalk an individual (Michigan Tech, (https://www.mtu.edu/deanofstudents/faculty-staff/intervention/resources/cyber-harassment/). Lastly, cyberbullying refers to bullying media with the use of digital technology through platforms or other internet services. It involves sharing harmful comments, posts and contents against a person.

Cyber Obscenities: This refers to the illegal trading of obscenity or pornography in cyberspace. Most times, cyber obscenity is used to refer to sexual crimes such as child pornography, ransoming nudity or nude images, pornography, and unprotected or hate speech against a gender/sex or sexual group.

Cyber terrorism: This is a criminal act perpetrated by the use of computers and telecommunication capabilities resulting in violence, destruction and/or disruption of services to create fear within a given population with the goal of influencing the government or population to conform to a particular political, social or ideological agenda (Cohen, 2014).

Scamming: This entails fraud and financial crimes or internet fraud. In this case, the victim divulges or shares his/her information with the other user known as the scammer. It implies a deceptive scheme or relationship aimed at defrauding unsuspected individuals or financial resources. Others include identity theft and invasion of privacy, hacking, counterfeiting and forgery, intellectual property theft, etc.

Challenges of Cyber Security in Nigeria

As recorded in the Nigerian Punch Newspaper, paypal.com reported that Nigerians lost about N159bn to cyber security in 2018 while commercial banks lost N15bn to electronic fraud and customers lost 1.9bn in the same year (Ogundepo, 2021). Nigeria is recorded as the 16th most vulnerable country to cyber attacks and this is despite its cybercrime prohibition and protection act or its increase in the global security index and its network readiness index. Nigeria ranked 47th on the global security index and the 4th African country recognised for its cyber security plan and policies. Still, it faces a myriad of cyber-attacks threatening both its business economy and the lives of its citizens.

We aim to highlight some of the challenges to a a sustainable cyber security framework in Nigeria, despite its investments over the years.

- Lack of security professionals: Cyber security is a growing field and it is pertinent to establish it as a workforce which can enable the recruitment of qualified professionals or adequate IT savvy graduates or professionals and build a future generation of security specialists.
- Lack of security education and trainings: Employees, security agencies such as the police and military as well as the public ought to be trained on the protection of information and data within cyberspace. This is because some of the breaches in the network systems are caused by human factors such as weak passwords, spam mail and external links in messages, etc. Once properly enlightened and trained, individuals can spot phishing and spamming attempts to reduce the risks of becoming a victim.
- High level of secrecy: When breaches occur, the majority of the corporations do not divulge information to the appropriate quarters nor inform members of their staff or customers. This high level of secrecy affects awareness of cyber crimes as customers are shareholders in that particular organisation and should be made aware of the risk to their properties, data or information.
- Exclusion and non-involvement of security outfits in cyber security: The security agencies such as the police and military are often excluded from activities relating to cyber security. They lack the technical know-how, expertise, experience and knowledge to probe into such issues.
- Lack of enforcement by the National Information Technology Development Agency in ensuring private companies report data breaches. Without the public's opinion, there is a lack of information for consumers/customers thereby, thwarting efforts to show the risks of cyber security to the general public

and how they can better protect themselves against it. When corporations do not report security leaks or breaches, how can the organisation of the government help in investigating and recovering lost sensitive data?

- Lack of a legal framework and legislation that identify and describe "illicit cyber activities", investigates them, prosecutes and enforces punishments to the degrees of the crimes committed.
- Lack of sustainable and efficient cyber security architecture, design and policies. Cyberlaw acts or agencies in Nigeria are mostly ineffective in investigating, detecting or recovering data or properties lost by victims or businesses. The majority of security networks in Nigeria are currently operating on old security designs that are vulnerable to attacks. Cyber security acts are, in some cases, not effective and their policies are not often implemented, effected or sustainable.

Security Challenges and Issues in Nigeria

Nigeria is battling threats on different fronts both traditionally, internally, externally and non-physically. The nation is currently home to a variety of criminal activities such as kidnapping for ransom, banditry, armed robbery, Fulani herdsmen/farmer clashes, and insurgent groups such as the Boko Haram and the Niger Delta Militants.

Kidnapping has become a new business for idle individuals. They target low-income, middle and high-income families and individuals with the aim of exchanging them for ransom. Citizens live in anxiety especially road travellers as transport buses are hijacked and passengers are taken; some are killed and others are exchanged for money.

In the conflict predating this period, the Fulani herders and farmers in different communities in the country began to engage in various conflicts. The conflicts between both groups were often over land and resources and had an economic, environmental and ethnic undertone. The herdsmen who moved their cows for grazing into farmlands and forests were reported to have damaged the crops of the farmers in the grazing process. Rather than reach an amicable resolution, it was reported that herders began to terrorise and harass members of the community which in turn led to clashes between both groups. This has been a cause of unrest among the Southwest and Eastern communities, thereby causing major loss of lives, properties and peace (Crisis Group 2018; Isola 2018).

Hunger and poverty, unemployment and corruption are at the tier of these threats to national security which also pose risks to national development. Perhaps if the government had been able to eliminate or reduce hunger and poverty in accordance with the United Nations Sustainable Development Goals (SDGs), then the rate of youths involved in criminal activities would be low. However, hunger, poverty and

unemployment are driving forces behind searching for alternatives to eliminating poverty within low-income households.

Educated and employable youths equipped with technical know-how in different fields and specialisations are on the streets. Take, for instance, graduates of computer science or computer engineering who are not gainfully employed; their talents could be discovered by criminals and used for other immoral purposes such as hacking or misuse of computer networking systems to the detriment of other members of the society.

Corruption is another serious problem facing Nigeria today. This is often a result of inefficient and ineffective leaders in public offices. Public servants in Nigeria are often after personal gains rather than upholding the duties of the offices they have been appointed to and do diligently serve the people. Corrupt practices in Nigeria include embezzlement of funds and national resources, non-commitment to citizens, lack of accountability, nepotism and many more.

The law enforcement agencies that have been created with the goal of protecting citizens are often found to be against the people, siding with corrupt public officers, receiving bribes, punishing or killing innocent citizens and so on. This further distances the people from reaching out to the nearest security outfit in case of crisis or clashes. Among the many consequences of the act of corruption and lack of commitment of the government to the concerns of the citizens is the lack of trust in the government as well as having low or no expectation for achieving results within their offices.

Even when crimes are detected, citizens have little or no trust that such crimes would be duly investigated and properties would be recovered or families compensated. This is because suddenly so-called reformed members of the northern terrorist Boko Haram group were released upon pleading for respite after their barbaric acts, and corrupt public officers were released after bail or fines. There is also the case of the Special Anti-robbery Squad (SARS) killing innocent youths and harassing citizens. Similarly, there is the case of the EndSARS protest of 2021 which called against police brutality and still citizens were allegedly killed. There are numerous security challenges facing Nigeria and the solution to these problems is not the millions of funds spent on ‘security’ but a reformation of the commitment of the government to the people and a re-assessment of leadership in the country.

It is our belief that when these challenges are addressed along with investment in adequate modern security technology, only then can cyber security be able to successfully contribute to the reduction and elimination of the high level of insecurity in the nation. Based on the foregoing, this paper advocates the need for the Nigerian government to invest in cyber security training and outfit not only to

ensure the protection of citizenry data, lives and property but also to strengthen the capacity of the existing security agencies in the country. The establishment of cyber laws, education, professionals and technology will improve security, aid peacebuilding and development in Nigeria.

Cyber-Security, Nation Building and Development in Nigeria

The importance of cyber security to nation-building and development cannot be overemphasised. The cyber environment is a global economy. More than 50 million Nigeria engage in online activities. Piggy Vest, appointments, travel bookings, and especially shopping for service, most of these activities are now carried out virtually. Many of our daily transactions, especially buying and selling online, are made through mobile phones, internet banking or E-wallets (Bitcoins, Opay, Palm pay, Paypal, etc).

Virtually everyone uses one computer or modern device or another. Even armed robbers communicate with digital tools, messaging, email or calls. The so-called insurgent groups such as the Niger Delta militants, who exploit, destroy and loot oil wells are individuals with a system of communication and electronic devices.

It is obvious that with the right security systems and tools, perpetrators can be traced, emails can be breached and this can aid effective security mechanisms in affected areas. Armed robbers, kidnappers and criminals use sophisticated devices that are mostly embedded with security chips by manufacturers or can be monitored and accessed by ethical hackers. The use of these computers and digital devices can decrease security threats and aid the restoration of peace and safety.

Cyber security has numerous benefits for the Nigerian economy and requires attention to safeguard the cyber environment from physical and digital threats and activities. Some of the ways we propose this can be done are for the government, individuals and business corporations too;

- Invest in modern security devices such as smart alarms and monitors, location tracking devices, surveillance systems, etc.
- Focus on identifying cyber security professionals and creating a workforce within governmental and corporate bodies.
- Develop strong security systems and cyber security architecture. Organisations should develop a security culture with a strong foundation of security systems to protect data, information and threats. Security systems should also be created with the aid of cryptography (decrypting and encrypting).
- Encourage skill acquisition programmes in the field of cyber security and information/network security.
- Hiring ethical hackers. Ethical hackers refer to certified ethical computer programmers or engineers with knowledge of computer systems to assess the weakness in a computer system or security design that can lead to hacking. Ethical hackers penetrate networks with the purpose of finding and fixing vulnerabilities using the same tools and knowledge as a malicious hacker but in a lawful and

legitimate manner to assess the security posture of a target system (Wikipedia, 2016).

- Funding and investment in modern technology such as voice recognition and authorisation software and applications, video surveillance systems and smart alarms, etc.
- Educating the security outfit agencies such as the police, robbery squad, special crimes unit and military. Also equipping them with up-to-date technologies such as body cams, drones, internet connectivity and remote access such as walkie-talkies and gears.

The core of criminal activities and insecurity is a lack of systematic and theoretical ethical structures. As such, from a philosophical and humanistic perspective, one major challenge for stabilising security and national development within Nigeria and cyberspace is a lack of moral and ethical education and policies and assessment of traditional and cultural history in regard to security.

Nigeria needs effective leaders that can successfully enact and likewise effect policies to safeguard its people. Nigeria is still suffering from a lack of ethical, effective and adequate leaders. Corruption is at the foundation of policies and laws; as such, it is most challenging to put into practice these numerous cyber laws and policies in a country filled with greedy and inefficient leaders.

Conclusion

Despite its innovative ventures and technology, modern-day technological tools have opened the world to a wide expanse of cyber-attacks and criminal activities. Cyber threats and attacks are detrimental to the security of any nation. In as much as society continues to rely on, use and engage in information technology and the use of the Internet for personal and corporate purposes such as communication and other activities, security and cyber threat will remain constant.

In order to address and mitigate the consequence of poor cyber security networks, technical measures must be put in place and the government, along with its security outfits and networks, ought to keep up with modern technological advancements and developments. It also requires the active input, commitment and funding from the government to create a security ICT workforce, build young security professionals and establish adequate frameworks guiding cyberspace as Nigeria is currently at an unfavourable disadvantage with respect to national security, and economic and socio-political development.

References

Australian Cyber Security Centre. https://www.cyber.gov.au/ac/acc/view-all-content/advice/cyber-security-principles. 28th February, 2022

Cohen, D. 2014. Cyber Terrorism. Cyber Crime and Cyber Terrorism Investigator's Handbook. https://www.sciencedirect.com/topics/computer-science/cyber-terrorism. 28th February, 2022.

Computer Security Resource Centre (CSRC NIST). Cyber Space. https://csrc.nist.gov/glossary/term/cyberspace#. Accessed 26th February, 2022.

Crisis Group. 2018. Stopping Nigeria's Spiralling Farmer Herders Violence. https://www.crisisgroup.org/africa/west-africa/nigeria/262-stopping-nigerias-spiralling-farmer-herder-violence. 26th February, 2022.

Gasser, M. 1988. Building a Secure Computer System (PDF). Van Nostrand Reinhold.

Isola, Olusola. 2018. Herdmen and Farmer Conflict in Nigeria: A Threat to Peace-building and Human Security in West Africa. https://africaupclose.wilsoncenter.org/herdsmen-and-farmers-conflict-in-nigeria-a-threat-to-peacebuilding-and-human-security-in-west-africa/. 27th February, 2022.

National Cyber Security Index (NCSI). https://ncsi.ega.ee/country/ng/. 28th February, 2022.

Michigan Tech. N.D. Cyber Harassment. https://www.mtu.edu/deanofstudents/faculty-staff/intervention/resources/cyber-harassment/. 28thFebruary, 2022.

Ogundepo, Janet. 2021. Nigeria to invest in Cyber security against spate of attacks. Punch

Newspaper. https://www.google.com/amp/s/punchng.com/nigeria-urged-to-invest-in-cybersecurity-against-space-of-attack/%3famp. Accessed 26th February, 2022

Puraji, Amaresh. Cyber Terrorism: World-wide weaponization. https://cii.in/webCMS/Upload/Amaresh%20Pujari,%20IPS5. 28th February, 2022

RSI Security. 2020. The purpose of cyber security architecture. https://www.google.com/amp/s/blog.rsisecurity.com/what-is-the-purpose-of-cybersecurity-architecture/amp/. 26th February, 2022

Vaughan, Jack. 2021. What is Data. https://www.techtarget.com/searchdatamanagement/definition/data, Retrieved 27th February, 2022.

Wikipedia. 2016. Certified ethical hacker. https://en.m.wikipedia.org/wiki/certified_ethical_hacker. 28th February, 2022