Cyber Threat to Critical Infracstructure and Defending National Security in Nigeria

International Journal of Economics, Business and Management Studies
Vol. 7, No. 2, 214-223, 2020
e-ISSN: 2226-4809/p-ISSN: 2304-6945

Gbenemene Kpae

University of Port Harcourt, Nigeria.
Email: Benkpae@hotmail.com

ABSTRACT

Cybercrime especially those that threatens critical infrastructures is a growing phenomenon in Nigeria, and posing great danger to the nation's national security. Prior to this time, cybercrime was limited to advance fee fraud with limited impact on the Nigeria's national security, however of recent cybercrimes have extended to other critical areas, such as finance, maritime, oil sector, telecommunication, defence etc that are vital for the survival of the nation's economy and national security. Apart from economic sabotage committed by internet criminals, terrorist organisations and individuals with subversive tendencies have also taken advantage of the weak enforcement of the regulatory framework in Nigeria to commit cybercrime. As many companies including government institutions are becoming digitalized, so cyber criminals are devising ways to attack the nation's critical infrastructures.. The long term impact of cybercrime on the nation's critical infrastructure is grave if the government does not take serious steps to tackle the problem. This paper examines the threat posed by cybercrime to Nigeria's critical infrastructure such as banking, information and telecommunication and national security.

Keywords: *Cybercrime, Critical infrastructure, National security, Banking, Nigeria.*
JEL Classification: *Cyber threat, Critical infrastructure.*

DOI: 10.20448/802.72.214.223
Citation | Gbenemene Kpae (2020). Cyber Threat to Critical Infracstructure and Defending National Security in Nigeria. International Journal of Economics, Business and Management Studies, 7(2): 214-223.

Funding: This study received no specific financial support.
Competing Interests: The author declares that there are no conflicts of interests regarding the publication of this paper.
History: Received: 16 September 2020/ Revised: 13 October 2020/ Accepted: 23 October 2020/ Published: 4 November 2020
Publisher: Online Science Publishing

Highlights of this paper

- This paper examines the threat posed by cybercrime to Nigeria's critical infrastructure such as banking, information and telecommunication and national security.

1. INTRODUCTION

"Our country will, at some point, face a major cyber event that will have a serious effect on our lives, our economy and the everyday functioning of our society." This grave warning came from the former United States Secretary of the Department of Homeland Security Janet Napolitano back in 2013 (Cisco, 2015). This is the same situation that Nigerian economy and national security is currently facing from cyber criminals. The availability of information and communication technology (ICT) has provided the means through which many Nigerians including private business owners have become victims of cyber-attacks. The rate of victimization to cybercriminals is further made easier with the availability of i-phones, tablets and other gadgets with internet accessibility. The reason why cybercrime has become such a serious problem in Nigeria is because most victims of cybercrime are left to bear the loss on their own with less support from the government and/or security agencies. Some private companies, particularly financial institutions, have increased their spending on cyber security, and sometime these companies transfer the cost of providing such security to their customers. National security is placed in serious jeopardy to cybercriminals as the prevalence of cybercrime puts the country in negative light and hinders foreign investment, and. also provides avenue for terrorist groups to spread their message of hate and secession in the country. Critical infrastructures are vital for the smooth running of every society, and their protection is one of the primary responsibilities of the government of any nation, because the disruption and destruction of these critical infrastructures would, definitely, hinder the growth and development of a nation. However, when these infrastructures are threatened by criminals particularly through a medium (internet) where there is very limited or probably inadequate policing, as the case in Nigeria, then the economy and national security is in grave danger. As many organizations in Nigeria, both public and private are increasingly using the internet, so they are becoming vulnerable to cyber-attacks.

The prevalence of cybercrime in Nigeria is due to several factors including unemployment, our materialistic culture, inadequate policing of the internet and lack of enforcement of the regulatory framework in Nigeria (Omodunbi, Diase, Olaniyan, & Esan, 2016). Other causes of cybercrime in Nigeria include poverty, corruption, urbanization, fallen moral standards, proliferation of cyber cafes and porous nature of the internet, gullibility, negative role model, and quick desire to make money without a corresponding emphasis for hardwork (Umaru, 2019). The impact of cybercrime on the society is that many Nigerians are losing millions of naira daily due to activities of illegal criminals operating just from the comfort of their homes. The overall consequences of this criminal behavior on the national economy is great because the financial institutions are losing billions of dollars to cyber criminals while citizens are afraid to transact businesses with unknown persons via the net. Apart from financial loss to banks, cybercrime retards economic development of the nation where this behavior is prevalent. More importantly, it destroys the image of the country which makes it difficult for foreign direct investment in the country. It also increases the operating cost of the financial institutions as they devote more of their profits to safeguarding the companies' network operating systems from cyber-attacks. This paper, therefore, investigates the impact of cybercrime on Nigeria's critical infrastructure such as banking industry, Information and communication, and national security.

2. LITERATURE REVIEW

2.1. Theoretical Review

Cybercrime and the threat this criminal behavior poses to critical infrastructure is anchored on Sykes and Matza (1957) theory of 'neutralization'. Just like Sutherland (1947) and Cressy (1960) Sykes and Matza believed that criminal behavior is learned through a process of differential association. Thus, in many ways their theory is seen as an expansion of Sutherland and Cressey's theory. Sykes and Matza, however, proposed a 'drift' theory (also known as neutralization theory), which differentiates their their own theory from that of Sutherland and Cressey. They hold that delinquents do not learn values that are completely counter to conventional society, rather, they generally disapprove of delinquency in the same way as conventional society. Instead, delinquents learn techniques of neutralization, which enable them to commit a delinquent act without viewing the act or themselves as truly delinquent. Techniques of neutralization include denial of responsibility, denial of injury, denial of victim, condemnation of the condemners, and appeal to higher loyalties (Iwarimie-Jaja, 2003). In Nigeria, most adolescent that engage in cybercrime will use two of Sykes and Matza neutralization techniques such as denial of responsibility and condemnation of the condemners. Many young people who engage in various crimes in Nigeria including cybercrimes simply argue that they are victims of a poorly mismanaged economy where there is no employment for the young people. This technique of neutralization simply makes the youths appear to be victims of circumstance, because if the government provided employment for the youths and cater for their needs then they would have been less likely to engage in criminal behavior. Another technique of neutralization adopted by most Nigerian youths that are involved in cybercrimes that affect our critical infrastructure is condemnation of the condemners. Most cyber criminals contend that those who condemn their behavior through the criminal justice system are also guilty of the same behavior, except that they do not get caught and punished because of their social class in society. When these two techniques of neutralization are adopted by most adolescents who engage in cybercrime, they do not see anything wrong in their criminal behavior. These two techniques are usually adopted by most adolescents who engage in crime in Nigeria especially cyber criminals. They see themselves as victim of society and a failed system that has not been able to provide for her young people, and believe that many of those who condemn them are also guilty of the same offence, but are not caught because of their privileged positions. As a result, most adolescents see their cyber criminality as a rebellion against the Nigerian society that has failed to provide or cater for them.

2.1.1. Growth of Internet Crimes

Cybercrime or internet crime is a criminal behavior that became known or common globally with the introduction information and communication technology. Alansari, Aljazzaf, and Sarfraz (2019) believe that internet crimes started first in the 1960s when disgruntle employees working in corporations started tampering with company computers for personal gains. But in the 1980s e-crime extended to physical damage to computers including writing of malicious software and self-implicating programmes to interfere with personal computers, Later on cybercrime was modernized by criminals who used unauthorized access to subvert security systems of companies for personal or monetary gains. However, as IT began to grow towards the end of the 1980s, cybercriminals started seeking for means to penetrate the system for amusements purposes. As internet network increased worldwide, several poorly monitored computers became vulnerable to sabotage, political action and financial gain. By early 1990s, there was increase in the use of computers to commit financial crimes by destabilization of computer system. The availability of mobile phones, particularly smart phones, and tablet PCs also saw increase in cybercrime (Alansari et al., 2019).

2.1.2. Cyber Crime in Nigeria

In Nigeria cybercrime started in the late 1990's among some youths especially university undergraduates. Subsequently, internet crime became popular among university graduates due to economic downturn occasioned by the high level of unemployment in the country and the quick handsome payoff associated with cyber fraud (Ezea, 2017). The strategy used by internet criminals then was to send fictitious mails to unsuspecting foreigners, mostly Americans, who want to invest in the Nigerian oil industry. These cyber criminals were ordinarily called 'yahoo' 'yahoo' boys in Nigeria. Cybercrime also became popular among the youths due to the weak enforcement of the criminal law against such behavior by law enforcement agents, so as to deter intending criminal offenders (Poroma, Kpae, & Abel, 2016). But this crime then was limited to foreign victims alone. However, today cybercrime has become very popular among the youths, particularly jobless graduates and majority of its victims are Nigerians. Cybercrime is made easier with the availability of smart phones with internet accesability. Cybercrime has become the quickest means for most unemployed youths to acquire material things that are highly cherished by the Nigerian society.

The problem right now is that cybercrime has been localized because majority of the victims are no longer foreigners located in countries, which are located on the web by the cyber criminals, but Nigerians who are going about in their daily business. One of the areas where this criminal behavior has been rampant is the banking sector. The banking sector in Nigeria depends on information processes supported by information and communication technology for their daily business operation, which makes them vulnerable to cyber-attacks. Because most financial institutions have become digitalized, cyber criminals have turned their activities from foreign nationals to Nigerians where people can be defrauded from their bank through the medium of Automated Teller Machine (ATM) cards, especially if they mistakenly let out their pin numbers to some unknown persons.

Cybercrime through the banks digital channels is becoming pervasive in Nigeria because, as the Nigerian economy is shrinking due to COVID 19 virus and fall in oil price, many financial institutions, in order to remain in business, are forcing their customers to make payments through one of their digital platforms such as quick teller, mobile application, ATMs, remittals etc. Apart from reducing the crowd in the banking halls, the banks are able to charge some fees for each transaction made by the customer outside of the banking halls. More importantly, by forcing their customers to use the e-channels for banking transactions, the banks' managements are also able to safe cost by reducing their staff strength. The problem is that as many customers are going digital particularly by using mobile phones to make online transfers so people are becoming victims of financial fraud from cyber criminals. In fact, as the number of telephone subscription increases in Nigeria from about 53% in 2015 to 84% in 2018, and about 24 million smart phone users so cybercrime is increasing (Adepetun, 2018). Presently, all the cyber hackers need is access to a customer phone sim card that is registered to an account for the victim to be defrauded of the entire amount he/she has in his account.

Due to the growing trend in cybercrime in Nigeria, cyber security has become imperative for the survival of our banks. But as many financial institutions are deploying more cost to ICT security, so cyber criminals are developing newer ways to attack their systems. For instance, the banking industry lost about 15.15 billion naira to cyber criminals and forgeries in 2018, about 539% higher than the figure recorded in 2017 (Adesoji, 2019). In fact, it is projected that by the end of 2020, global Cyber security spending will reach $170bn, a 126% increase from $75bn in 2015 (Umaru, 2019).

As a result of the high rate of cybercrime in Nigeria, development of a comprehensive policy framework on Critical Infrastructure Protection (CIP) is very essential for the survival of the national economy and national security. Therefore, exposure of our financial institutions to cyber-threats by cyber-criminals and citizens to cyber-terrorism is a serious threat to our economy and national security. Additionally, the inability of the government to adequately police the internet also exposes our national security and defence to regular threat by terrorists.

Another critical infrastructure that has been impacted by cybercrime is information and communication technology (ICT). As the globe is becoming a global village with the availability of ICT so cybercrimes that were never imagined before are beginning to spring up. Criminal behavior such as spamming, credit card frauds, ATM frauds, phishing, identity fraud, and terrorism are common with the introduction of ICT. In fact, terrorist groups have exploited the ICT to their own advantage. For instance, terrorists and terrorist organisations exploit the internet and social media not only to commit serious acts of terrorism, but also facilitate a wide range of terrorist activities, including incitement, radicalization, recruitment, training, planning, collection of information, communication, preparation and financing (Security Council: Counter-Terrorism Committee, 2019). In response to increasing level of cyber threats and global cyber terrorism, in 2017 Facebook, Microsoft, Twitter and You Tube announced the formation of the Global Internet Forum to counter-terrorism. The initiative was part of the United Nation's strategy to get the private sector involved in the fight against terrorism and violent extremism using the ICT. Despite how laudable this initiative was, terrorist groups have always found a way to abuse the ICT especially social media. The overall effect of this behavior is that national security is threatened as the nation is constantly exposed to the activities of terrorist groups and individuals with subversive tendencies.

2.2. Conceptual Review

2.2.1. Cyber Crime

According to Umaru (2019) the word 'cyber' is derived from the word 'cybernetics' which means or refers to the science of communication, which deals with the study of automatic control system as well as the mechanical electrical communication systems. Thus cyber is used to describe interactions among computer networks. Crime on the other hand has to do with act or omissions that are injurious to society that is punishable by law.

Cybercrimes are offenses that are committed against individuals or groups with a criminal motive of intentionally harming the reputation of the victim, causing physical or mental harm, and cause loss of money or information directly or indirectly by using internet and electronic devices (Alansari et al., 2019). Specifically, cybercrime is a crime committed by criminals who make use of the computer as a tool and the internet as a connection to commit a lot of internet related offences such as illegal downloading of music files and movies, piracy, spam mailing, etc (Omodunbi et al., 2016).

2.2.2. Cyber Crime and National Security

Cybercrime has already been defined above as crime related to the internet, while national security is the ability of a state or nation to protect her citizens from any kind of threat both internal and external (Osisanya, 2020).

The main responsibility of a state is to protect its national interest through the wellbeing of its citizen, which therefore constitutes its national security. The advent of ICT, prompted many states to depend on the internet for their everyday operation and to enhance their national security. The problem is that if the government data base were to be compromised through hacking, then the nation's security would be in serious jeopardy.

The relationship between cybercrime and national security is that while the state seeks to protect itself and citizen's wellbeing against multidimensional threats, cybercrime targets the nation or its citizen through communication device or internet. Cybercrime has several effects on national security including economic sabotage, negative international image, and threat to lives.

2.2.3. The Concept of Critical Infrastructures

A critical infrastructure is a network or system which is vital for an organization, society or economy day-to-day operations. They may include electricity, gas, oil production, telecommunication; water supply, agriculture, hospitals, transportation systems (like railways, airports, etc.); banking and other financial services; people security services. In the U.S., the concept of critical infrastructure has gone beyond infrastructures whose prolonged unavailability could cause significant military and/or economic disruption to include attacks on national monuments, where an attack can alter the proper functioning of a factory and threaten the safety of surrounding communities (Patrascu, 2012). Hebar and Zarsky (2017) believe that the intentional actions of human adversaries as part of armed or unarmed conflicts between nations, criminal activities (including various types of hacking), revengeful measures of disgruntled employees, or acts of terrorism pose a substantial threat to critical infrastructures.

2.2.4. Cyber Terrorism

Cyber terrorism is one of the cyber threats that most Nigerians have been victim of especially with radical Islamic movement and Boko Haram insurgency going on in the North, and Indigenous people of Biafra (IPOB) separatist group in the south east. Both have depended heavily on information technology to propagate their messages, either about strict enforcement of sharia law in northern Nigeria or separation of the Nigerian state. Cyber terrorism (CT) consists of using computer time to advance one's political or ideological ends. CT is another area where cyber threat has become commonplace as a result of the availability of the internet. Similarly, terrorism is one of the crimes that have become prevalent as a result of the availability of ICT. Terrorism is defined as the use or the threat of the use of violence, a method of combat, or a strategy to achieve certain targets. Its aim is to induce a state of fear in the victim that is ruthless and does not conform to humanitarian rules and to create publicity to its course (Casin, 2018). Bruce Hoffman in Gluschke, Casin, and Macori (2018) defines terrorism as "the deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change**. C**yber terrorism is the use of cyber capabilities to commit terrorism. More specifically, "cyber terrorism is the use of cyber capabilities to conduct enabling, disruptive, and destructive militant operations in cyberspace to create and exploit fear through violence or the threat of violence in the pursuit of political change". Cyber terrorism can also include attacks on internet businesses, but when this is done for economic motivations rather than political ones, it is to be regarded as cybercrime. Cyber terrorism is limited to actions by individuals, independent groups, or organizations. Any form of cyber-attack conducted by governments and nation states may be defined as cyber warfare.

According to the US Federal Bureau of Investigation (FBI), cyber terrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents. Unlike a nuisance virus or computer attack that result in a denial of service, a cyber-terrorist attack is designed to cause physical violence or extreme financial harm. According to the US Commission of Critical Infrastructure Protection, possible cyber terrorist targets include the banking industry, military installations, power plants, air traffic control centers, and water systems.

The goal of terrorists in using destructive cyber militancy (DeCM) is to manipulate computer code and corrupt information system functions in order to damage or destroy virtual and/or physical assets. Manipulating or corrupting information may, at a minimum, generate misinformation and induce confusion and loss of confidence in critical systems. In the worst case, DeCM may cause catastrophic effects on critical infrastructure, possibly resulting in death and destruction. DeCM activities are often described in the literature as "pure" cyber terrorism, which is the direct use of cyber hardware, software, and networks to create kinetic effects on par with traditional acts of terrorism, as opposed to merely using information communication technology in support of organizational communication and "traditional" terrorism. Most experts in the field narrowly define cyber terrorism to include only the direct use of cyber capabilities, as opposed to activities in support of terrorism (Macori, 2018).

There are two close connections between the internet and terrorism. The internet has become a forum for terrorist groups and individual terrorists to spread their message of hate and violence, as well as to communicate with one another. For instance, the Boko Haram insurgents in Nigeria have used the internet to communicate with one another and to share video clips of their attacks on government forces. Second, individuals and groups have tried to attack computer networks, including those on the internet, which are known as cyber terrorism or cyber warfare (Eleonora, Loi, & Vaghmaei, 2019). A critical problem that has been identified in cyberspace is the inability of businesses and private companies to share information with the government. This causes insufficient information, skews analysts' result, and prevents the state from collecting adequate data on cyber-attacks and developing better defences against such attacks (Eleonora et al., 2019).

2.2.5. Critical Infrastructure and National Security in Nigeria

The question as to what constitute critical infrastructure (CI) vary from country to country, but in simple term, critical infrastructures are generally understood as facilities and services that are essential for the basic operations of a society (Sandsolz, 2017). In the U.S., critical infrastructure describes the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on the physical or economic security or public health or safety of that society (Hemme, 2015). According to Alcaraz and Zeadallly (2015) critical infrastructure (CI) consist of a set of system, whether physical or virtual so essential to a nation that any disruption of it could have serious impact on national security, economic well-being, public health, or any combination of these.

Globally there is consensus that the following sectors fall under the ambit of critical infrastructures, they include, energy, water, telecommunication, transportation, healthcare, banking and finance. In Nigeria, for instance, sectors such as the oil and gas, maritime, banking and finance, transportation, telecommunication and defence are considered critical infrastructures; in which case, any problem or disruptions of any of these sectors would definitely affect the country's economy and national security. The focus of this paper, however, is on banking and finance and telecommunication, and security sectors. The banking sector is so critical to the Nigerian economy, as more people are turning to online banking for their daily transactions so their bank accounts are becoming vulnerable to cyber criminals. On daily basis, millions of naira are being withdrawn from people's account without their knowledge. These online frauds are facilitated by telecommunication especially mobile phones which are connected to peoples' accounts. In fact, the availability of online banking and telecommunication have made it easier for cyber criminals to defraud peoples' accounts just from the comfort of their homes without police detection and apprehension.

Apart from the banking and finance sector that have become vulnerable to cyber-threats, the telecommunication sector is another critical sector exposed to cyber criminals. The telecommunication companies provide the internet services for both the public and private sectors. They provide the internet for public users and through its services the public can access information, particularly social media through their mobile phones. As a result, people become exposed to cyber-attacks through their cellular phones. For instance, many people especially females are exposed to cyber stalking while on the net. Similarly, many people with seditious tendencies have used the internet particularly social media to engage in cyber terrorism by sending divisive messages to people propagating the division of Nigeria either on ethnic or religious lines. For example, the Boko Haram insurgency and the IPOB have relied heavily on the social media to propagate messages of hate and attacks on government forces engaging in counter-insurgency. While these messages have not succeeded in braking up Nigeria, but they have succeeded in radicalizing Islamic fundamentalist and rallying support and sympathy from members of the public, especially youths to their course.

2.2.6. Legislative Frameworks for Protecting Critical Infrastructure

The Nigerian government has passed numerous legislations in an effort to fight cyber-crimes including the most recent, the Cybercrime Act of 2015 that prescribes ten million naira fine or five years imprisonment for hackers, Apart from this legislation, there are other laws that govern cyber-crimes in Nigeria such as the Advance Fee '419' or section 419 of the criminal code, Advance Fee Fraud and other related offences degree, the Money Laundry (Prohibition Act), and the Economic and Financial Commission (Establishment Act) of 2004. However, despites these legislations, cyber-crimes continue to thrive in Nigeria (Salu, 2004).

In the U.S, in 2018, the government under Donald Trump signed into law the Cyber Security and Infrastructure Security Agency Act which establishes the Cyber Security and Infrastructure Security Agency (CISA). The purpose of the CISA is to coordinates security and resilience efforts using trusted partnership across the private and public sectors, and deliver technical assistance and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide. Further, the European Union (EU) through its European Programme for Critical Infrastructure Protection (ECIP) has also developed a legislative framework for the protection of critical infrastructure among its member countries.

2.2.7. Problems of Enforcement of Cyber Attacks and Consequences in Nigeria

Law enforcement agencies face a variety of enforcement difficulties, particularly in locating the online criminals. Cyber-attacks can occur beyond the sovereignty of the state, so the culprit does not need to escape and thus has fewer risks. Cyber-attacks also raise an 'attribution problem. Attackers use digital technology to cover their tracks or even implant false and deceptive identification marks. In many instances, the attacker's true identity is protected because she uses a public or 'zombie' computer belonging to another. All of these elements minimize the chances of attackers getting caught, thus improving the attackers' capabilities to attack and enhancing the threat of their actions (Hebar & Zarsky, 2017).

The cyber realm also enhances the accessibility of threatening tools and measures. Equipped with the correct set of skills, almost anyone, from any place, can execute an attack, using even public computers. Contrast this with physical attacks, which usually require purchasing or concocting explosives or other weapons, which are not as widely available as computers. Furthermore, digital weapons can usually be purchased on black markets and attacks ordered via more secured communications. Cyber conditions therefore increase the set of potential attackers and thus the threats they generate.

As is previously noted, cyber-attacks are often difficult and expensive to detect and attribute to one specific attacker. These factors render such attacks more dangerous, as their outcomes could be dire for several reasons. Cyber at1tacks—as opposed to kinetic destruction—could remain undetected for an extensive period of time. The passage of time allows the attacker to cause even greater harm. Furthermore, when intrusion into the CI remains undetected, the attacker can execute the attack at any time—usually the point at which the greatest damage will be caused. Finally, the attack might never be detected if the damage and disruption it caused is attributed to a malfunction. This oversight allows the attackers to repeat their actions at a later time, causing even greater harm.

3. METHODOLOGY

The nature of the data used for this study was purely qualitative and secondary data, whereby information was sourced from academic journals, internet publications, newspapers and magazines. This information provided a useful source of data for the research.

4. CONCLUSION

Critical infrastructures are very vital for the survival of any nation, and any attack or tampering with their smooth running will definitely affect the economy and national security of that society. Infrastructures that rely on networking are the most vulnerable to cyber threat and attacks. In Nigeria, while sectors such as oil and gas, transportation, communication, and maritime are susceptible to cyber-attacks, but the banking sector and national security are the most vulnerable to cyber criminals. Daily, many Nigerians are victims of cyber criminals as their monies are electronically removed from their bank accounts by unknown persons. Further, terrorist organizations and individuals with subversive tendencies have taken advantage of the weak policing of the internet in Nigeria to commit cybercrime by sending divisive messages to individuals. As many organisations (both public and private) are depending on information technology for their operation, the government must develop a comprehensive framework by ensuring that people's personal data and critical infrastructures are protected from sophisticated cyber criminals and provide cyber security for the nation's critical infrastructure networks. Apart from cyber security of critical infrastructure against cyber threat, there should be synergy between the government and private organizations through network policing to ensure that cyber criminals are apprehended and prosecuted, so as to serve as deterrence to others. More significantly, the government should ensure that young people are provided with employment so as to discourage the urge for them to engage in cybercrime. Lastly, the government should sensitize the people through the mass media on the significance of protecting their phones against cyber criminals.

REFERENCES

Adepetun, A. (2018). Nigeria mobile phone penetration hits 84 percent. The Guardian.Retrieved from: www.guardian.ng. Acessed 9/6/2020.

Adesoji, B. S. (2019). Banks lost N15billion to fraud and cyber crime in 2018. Business News. Retrieved from: www.nairametrics.com. Acessed 5/9/2020.

Alansari, M. M., Aljazzaf, Z. M., & Sarfraz, M. (2019). On cyber crime and cyber security. In M. Sarfraz (Ed.), Development in information technology and cybernetic wars (pp. 1-41). Hershey, PA. USA: IGI Global.

Alcaraz, C., & Zeadallly, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st Century. *International Journal of Critical Infrastructure Protection (IJCIP), Elsivier Science, 8*, 1-35.

Casin, M. H. (2018). *Cyber security policies and critical infrastructure protection*: Institute for Security and Safety Press.

Cisco. (2015). Addressing critical infrastructure cyber threats for State and Local Governments: Application of a Threat-Centric Approach through the NIST cybersecurity framework.

Cressy, D. R. (1960). The theory of differential association: An introduction. *Social Problems, 8*(1), 2-6.

Eleonora, V., Loi, M., & Vaghmaei, E. (2019). Cybersecurity of critical infrastructure. *In The Ethics of Cybersecurity.*

Ezea, S. (2017). Prevalent of internet fraud among Nigerian youth. *The Guardian.*

Gluschke, G., Casin, M. H., & Macori. (2018). *Cyber security policies and critical infrastructure protection.* Germany: Institute for Security and Safety Press.

Hebar, E., & Zarsky, T. (2017). *Cyber security for infrastructure: A critical analysis* (Vol. 22). Florida State: University Law Review.

Hemme, C. (2015). Critical infrastructure protection: Maintenance is national security. *Journal of Strategic Security, 8*(3), 26-39.

Iwarimie-Jaja, D. (2003). *Criminology the study of crime.* Owerri: Springfield Publishers.

Macori, M. (2018). *The threat of cyber terrorism-a risk management perspective. In Gluschke et al. (2018) Cyber Security Policies and Critical Infrastructure Protection*: Institute for Security and Safety Press.

Omodunbi, B. A., Diase, P. O., Olaniyan, O. M., & Esan, A. O. (2016). Cyber crime in Nigeria: Analysis, detection and prevention. *FUOYE journal of Engineering and Technology, 1*(1), 2579-0617.

Osisanya, S. (2020). National security versus global security. *UN Chronicle.*

Patrascu, A. (2012). Cyber security evaluation of critical infrastructures system. Retrieved from: http//www.Research Gate.

Poroma, C. L., Kpae, G., & Abel, E. (2016). Youth unemployment and cybercrime in Port Harcourt Metropolis. In social insight. *Journal of the Association for the Promotion of Social Education in Nigeria, 15*(8), 69-81.

Salu, A. O. (2004). Online crimes and advance fee fraud in Nigeria – are available remedies adequate? *Journal of Money Laundering Control, 8*(2), 159- 167.

Sandsolz, S. (2017). Five things that you need to know about critical Infrastructures: United Nations University. Institute for Environment and Human Security. Retrieved from: http//:ehs,unc.edu/blog.

Security Council: Counter-Terrorism Committee. (2019). Information and communicatinn Technologies (ICT). Retrieved from: http//www.un.org/sc/ctc/focus-area/information-and-communication-technologies.

Sutherland, F. (1947). *Principle of criminology* (4th ed.). Philaldephia: Lippincott.

Sykes, & Matza. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review, 22*(6), 664-670.

Umaru, I. (2019). The impact of cybercrime on Nigerian economy and banking system. Retrieved from: http//www.ndic.gov.ng/wp-content.

Online Science Publishing *is not responsible or answerable for any loss, damage or liability, etc. caused in relation to/arising out of the use of the content. Any queries should be directed to the corresponding author of the article.*