Nigerian Journal of Arts and Humanities (NJAH), Volume 4 Number 1, 2024 (ISSN: 2814-3760, E-ISSN: 2955-0343)
NnamdiAzikiwe University, Nigeria, Indexed in Google Scholar (Email:njahjournal@gmail.com)

ISSUES IN CYBER-SECURITY ADMINISTRATION: LESSONS FROM DEVELOPING COUNTRY LIKE NIGERIA

Diyoke Michael Chika
Department of Sociology/Anthropology, Nnamdi Azikiwe University Awka, Nigeria
&
Ogboke, Eberechukwu Odichinma
D*epartment of Sociology/Anthropology, Nnamdi Azikiwe University, Awka, Nigeria*
&
Awogu Charles Olisa
Department of Sociology/Anthropology, Nnamdi Azikiwe University Awka, Nigeria

Abstract

Today almost all modern services rely on the usage of ICTs, including electricity generation, transportation networks, military forces, and logistics. However, the increasing dependence on ICTs makes service providers more vulnerable to attacks against vital infrastructures. Thus, it was on this note that this paper was set up to explore the issues in cyber-security administration from the prism of developing countries nay Nigeria. The methodology was based on a review of published articles, books, and journals to conclude the contemporary issues and challenges militating cyber security administration. The paper argued that while the ICT sector is in constant advancement, the volume and sophistication of cyber-attacks are also increasing. As a result, many government institutions face challenges in controlling cyber-attacks. It was further argued among others that the Nigerian National Cyber Security Policy and Strategy possess the required contents expected to be typically contained in such document, unfortunately, certain aspects that appear to be critical to the Nigerian scenario such as an explanation of the current national cyber security state, partnership with internet service providers, the establishment of digital identity frameworks, etc. were utterly absent. The paper concluded that given the growing sophistication of cyber-attacks, cyber security is a necessary consideration for individuals, businesses, and governments. Thus the paper recommended (amongst others) that the process of cyber security is continuous; it must be continuously updated. As new programs and cyber intruders develop and exploit new vulnerabilities in computer programs and systems, the relevant stakeholders and defenders have a continuous struggle to defeat their attempts.

Key Words: Cyber Security, Cyber Crime, Administration, Issues & Developing Countries

Introduction

Today the Internet is one of the fastest-growing areas of technical infrastructure development. Information and communication technologies (ICTs) are already pervasive, and the trend toward digitalization is accelerating. The growing demand for internet and

electronic access has led to the integration of computer technology into things that could not previously exist without it, such as vehicles, aviation services, energy supplies, water and communication services, and buildings. Almost all modern services rely on the usage of ICTs, including electricity generation, transportation networks, military forces, and logistics. According to Ravi (2012), every country's businesses and individuals rely on information and communication technology for their daily operations; computers are used to store data, process data, and generate reports. ICTs' impact on society extends much beyond the creation of fundamental information infrastructure and services.

Access to information and communication technologies (ICTs) has become a pillar for the development, availability, and use of network-based services. E-mails have displaced traditional letters; online web-based representation is now more essential to businesses than printed advertising materials and Internet-based networking and telecommunications services are growing at a quicker rate than landline communications (Gercke, 2012).

ICT technologies such as e-government, e-commerce, e-education, e-health, and e-environment are seen as growth enablers because they offer an effective platform for delivering a wide variety of critical services in remote and rural areas. ICT applications can help developing countries reach sustainable development by reducing poverty and strengthening health and environmental conditions. Investments in ICT applications and software will increase efficiency and output if the right strategy, context, and deployment processes are used.

While the ICT sector is constantly advancing and technological developments are being recorded, the volume and sophistication of cyber-attacks are also increasing; the sustained integration of ICTs into daily life appears to continue. Increasing dependence on ICTs makes service providers more vulnerable to attacks against vital infrastructures (Goodman, 2011). Even brief service interruptions could result in significant financial losses for e-commerce businesses. It is not just civil communications that could be disrupted by attacks; the reliance on ICTs is a significant factor risk for military communications. As a result, serious attention must be paid to the protection of personal or business information transmitted in cyberspace, as this has an impact on national security. Cyber threats are now the most effective way to attack an organization or a country, and the fact is that those with

malicious intent are finding ever more sophisticated ways to carry out their activities (Ravi, 2012).

For example, Twitter was the victim of a humiliating cyber-attack on July 17th, 2020. Hackers gained access to a number of verified accounts of well-known people, including Bill Gates, Jeff Bezos, and Elon Musk, and sent out tweets offering to deliver $2,000 worth of bitcoin to an anonymous bitcoin wallet for every $1,000 sent. Over $100,000 in donations were made in a short time since the wallet link was established. Jack Dorsey, Twitter, called it a "tough day." "This has happened, we all feel terrible," he wrote in a tweet. Twitter's attack is a harsh reminder that cyber-attacks are a major issue and threats are on the rise. But it allows businesses to be able to make these attacks known and help to counter them (Iyengar, 2020).

Earlier in 2003 alone, malware caused losses of up to USD 17 billion. According to some estimates, profits from cyber crime exceeded USD 100 billion for the first time in 2007, outstripping the illicit drug trade. About 60 percent of companies in the United States claim that cyber crime is more expensive to them than physical crime. These figures clearly illustrate the value of information security.

As a result, the International Telecommunications Union (ITU) and the International Multilateral Partnership Against Cyber Threats (IMPACT) signed an agreement on September 3, 2008, providing IMPACT with the Global Cyber Security Agenda (GCA), which provided expertise and tools to over 193 ITU Member States and formally to IMPACT in two years. The alliance specializes in aiding nations that lack the financial and technical capacity to establish their own cyber response centers. The ITU Regional Cyber Security Center (ITU-RCC) for the Arabian Peninsula has been created, and the Commission is recommending that the ITU Regional Cyber Security Center for the African Peninsula be hosted and managed in Nigeria. The idea by the ITU and IMPACT to build Cyber Security Centers throughout the world is an excellent way to tackle increasing global cyber security threats.

Many government institutions, particularly in third-world countries, face challenges such as inadequately secured infrastructure, a lack of awareness, and competing for financial and resource demands. More importantly, governments around the world store vast amounts of personal data and documents for their citizens, as well as secret government material,

making them a frequent target for hackers. Improved security helps government agencies provide trustworthy services to the public, preserve citizen-to-government communications, protect secret information, and ensure national security.

Unfortunately, Nigeria is not immune to cyber crime, as it has had its fair share of cases. Nigeria's cyber crime statistics are high and rising. The country is known for being a sanctuary for the commission of computer-aided advanced fee fraud, commonly referred to by the public as "419" or "yahoo-yahoo," among other crimes. The long-term commitment of these crimes has made Nigerians and foreigners alike extremely cautious, to the point that lawful contacts of all kinds originating in, or involving, Nigeria and throughout cyberspace are increasingly marked by rising skepticism (Olasanmi, 2010).

In addition, cyber-attacks are seldom revealed in developing countries like Nigeria, creating a sense of security. Nigeria, in reality, is suffering from some of the continent's worst cyber-attacks. According to a study conducted by Sophos, a cyber-security firm headquartered in the United Kingdom, 86 percent of Nigerian firms polled has experienced cyber-attacks in the previous 12 months, second only to India. More significantly, the country was in the top five in the world for major attacks such as malware, ransomware, stolen account passwords, and crypto-jacking. In Nigeria, misconfiguration of the organization's server has been used in 64% of cyber-attacks. Nigerian companies have had the highest data breaches of any of the countries assessed in the research. According to Diyoke & Edeh, (2020) in 2019 The National Information Technology Development Agency (NITDA) was reliably informed and duly confirmed that the Lagos State Internal Revenue Service (LIRS) published a web portal -https://lagos.qpay.ng/TaxPayer- where personal information of Lagos State taxpayers was gleaned by the general public in violation of the Nigeria Data Protection Regulation Act (NDPR). In the previous year, 57 percent of Nigerian businesses revealed that their public cloud data had been compromised. Meanwhile, 46% of Nigerian companies have disclosed that their account credentials, a tactic used by hackers to target Twitter, have been compromised in the previous year. Although Sophos captured these types of attacks, other attacks such as brute force, email hacks, the hijacking of Whats-App accounts, and many others, are indeed real threats (Adeyemi, 2020).

A 2014 report (supported by McAfee) projected that cyber crime costs the world economy $445 billion per year. A 2016 report by Cyber security Ventures anticipated that

global cyber crime damages will cost up to $6 trillion per year by 2021 and $10.5 trillion per year by 2025. In the United States, online credit and debit card theft cost $1.5 billion in 2012. In 2018, research conducted by the Center for Strategic and International Studies (CSIS) in collaboration with McAfee found that cyber crime costs approximately one percent of worldwide GDP, or $600 billion, each year. According to the World Economic Forum's 2020 Global Risk report, organized cyber crime groups are banding together to carry out illicit acts online, with the chance of discovery and punishment in the United States estimated to be less than 1% (World Economy Forum, 2020).

Thus, strengthening cyber security and sustaining vital information infrastructures are critical to any country's security and economic well-being. Making the Internet safer (and securing Internet users) has been an important part of the growth of innovative services as well as government policy (International Telecommunications Commission, 2011). Deterring cyber crime is an important part of a national strategy to secure cyber security and vital information infrastructure, and it necessitates, in particular, the implementation of effective legislation against the abuse of ICT for criminal or other purposes. It is against this background this paper was set to appraise in critical terms the issues and challenges of cyber security administration particularly in third world countries like Nigeria.

Conceptual Issues

Cyber Security and Cyber Crime

In today's linked world, cyber security and cyber crime are concerns that cannot be isolated from one another. The fact that cyber crime is included as one of the major challenges in the United Nations General Assembly resolution on cyber security from 2010 demonstrates this.

For example, Farhat, (2011) describes a cyber-crime as a computer-initiated assault against a website, a computer system, or a personal computer (collectively, a single computer) that jeopardizes the computer's confidentiality, integrity, or availability. In addition, the crimes come in the following forms: Unauthorized access to a computer system or its data; Unwanted disruption or denial of service attacks, including the takedown of entire web sites; Installation of viruses or malicious code (malware) on a computer system; Unauthorized use of a computer system for processing or storing data; Changes to the characteristics of a computer system's hardware, firmware, or operating system.

419 emails and letters, advance fee fraud, online auction fraud, online betting fraud, botnet-related fraud, child pornography, and related offenses, computer hacking, computer-related forgery, computer-related fraud, cracking, credit card fraud, cyber-laundering, cyber-smearing, cyber piracy, and cyber squatting are just a few examples of cyber crime. Others include intellectual property fraud, malware, viruses, misuse of devices, phishing, proxy servers, racist and xenophobic offenses, smishing, spamming, spoofing, Trojan horse, spyware, system interference, and vishing. Many sovereign countries have laws in place to prevent, monitor, criminalize, investigate, and punish cyber crime, and those that don't are working to enact legislation to address the problem.

On the other hand, according to Schatz, Bashroush & Wall, (2017) cyber security, also known as information technology security (IT security), is the protection of computer systems and networks against data leakage, unauthorized access, theft, or damage to hardware, software, or electronic data, as well as service disruption or misdirection. The field is becoming more important as people become more reliant on computer systems, the Internet, and wireless network standards like Bluetooth and Wi-Fi, as well as the proliferation of "smart" devices like smartphones, televisions, and the various devices that make up the "Internet of things." Schatz, Bashroush & Wall, (2017) further observed that due to its complexity cyber security is one of the major challenges in the modern world, both in terms of politics and technology.

Earlier, The International Telecommunications Union, (2011) describes cyber security as a collection of tools, regulations, protection principles, security protections, advice, risk management techniques, acts, training, best practices, insurance, and technology that can be used to secure the cyber environment, as well as the organization and properties of users. Linked computer devices, employees, infrastructure, programs, utilities, telecommunications networks, and the whole of knowledge transferred and/or processed in the cyber world are all examples of organizational and consumer assets. Thus, cyber security strives to guarantee that the organization's and users' security properties are satisfied and protected in the face of associated security risks in the cyber environment.

Cyber security is critical to the continuing growth of information technology and Internet services. Thus, improving cyber security and safeguarding vital information infrastructure is crucial to any country's security and economic well-being. Making the

Internet safer (and safeguarding Internet users) has become an essential component of the creation of new services as well as government policy. As a result, it's no surprise that cyber security has risen to the top of governmental priorities in a number of countries around the world, furthermore, it also ignited national cyber security policies that have sprung all over the world, as seen in several countries across the globe.

It was in this light that the Nigeria National Cyber security policy, (2014) provides a cyber-security vision/administration that is anchored on safe, secured, vibrant, resilient and trusted community that provide opportunities for its citizenry, safeguard national assets and interests, promote peaceful interactions and proactive engagement in cyberspace for national prosperity (National Cyber security Policy, 2014).

Cyber crime prevention is an essential component of national cyber security and critical information infrastructure protection plan. This involves, in particular, the implementation of suitable legislation prohibiting the use of ICTs for criminal or other objectives, as well as actions that threaten the integrity of national essential infrastructures. At the national level, this shared duty necessitates concerted effort on the part of government authorities, the business sector, and people in terms of incident prevention, preparedness, reaction, and recovery. Cooperation and coordination with appropriate partners are required at the regional and international levels.

Issues and Challenges in Cyber Security Administration

The Global Dimension

Unlike other kinds of crime, cyber crime routinely has a unique and pervasive global dimension. For instance, e-mails with illegal content frequently pass through a variety of countries during the transfer from sender to recipient, or illegal content is stored outside of the country, therefore close cooperation between the countries involved is critical in cyber crime investigations and preventions. However, existing mutual legal support arrangements are based on formal, complex, and often time-consuming protocols, and they frequently do not cover computer-specific investigations and prosecutions. Establishing procedures for rapid response to incidents, as well as requests for international cooperation, is thus critical (Clark, 2005).

Mutual legal assistance regimes in a number of countries are founded on the concept of "dual criminality" (Schjolberg, 2005). Put differently global investigations are generally limited to acts that are criminalized in all participating countries. Although most nations have a number of violations that can be penalized, such as the distribution of child pornography, regional differences have a significant role. Another example is different types of prohibited material, such as hate speech.

Many data transmission activities have an influence on countries other than their own. If direct links are temporarily unavailable, Internet data transport protocols rely on optimal routing. Despite the fact that domestic transfer operations inside the source country are limited, data can leave the country, be routed through routers outside the country, and then redirected back into the country to its final destination. Furthermore, many Internet services are dependent on services from other countries; for example, host providers may rent out web space in one nation based on hardware in another. An example that easily comes to mind in Nigeria is the current banning of the tweeter by the federal government of Nigeria citing a litany of problems with the social micro-blog in Nigeria, where misinformation and fake news spread through it have had real-world violent consequences.

Therefore, Keizer, (2005) argues that offenders or targets may be located in other countries; cyber crime investigations need the collaboration of law enforcement officials from all countries concerned. However, national sovereignty does not permit investigations within the territory of other nations without the consent of local authorities. Cyber crime investigations necessitate the cooperation and participation of authorities in all nations concerned. On the other hand, it is impossible to build cyber crime collaboration on standard mutual legal aid grounds because formal procedures and the time required to engage with foreign law enforcement organizations sometimes impede investigations. Investigations are frequently conducted in extremely short time frames. Data critical to locating offenders are frequently destroyed after only a short period of time. Because typical mutual legal help regimes require time to arrange, this short inquiry period is problematic (Gercke, 2006).

Again, if the offense is not criminalized in one of the countries involved in the investigation, the principle of dual criminality poses additional challenges as offenders may purposefully include third countries in their attacks to make the investigation more difficult (Atherton, 2010). Criminals may purposefully choose targets outside their own country and

act from countries with insufficient cyber crime legislation. The G8 24/7 Network and the requirements relating to international collaboration in the Council of Europe Convention on Cyber crime are two ways to increase the timeliness of international cooperation in cyber crime investigations.

Conversely, BinaKotiyal & Goudar, (2013) argued that developments resulting from technical standardization emanating from computer systems and mobiles gadgets could lead to the harmonization of national laws. For instance, aside from language differences and power adapters, there is very little difference between computer systems and mobile phones sold in Asia and those sold in Europe. Computer technology is essentially the same throughout the world. As a consequence of standardization, the network protocols used in African countries are also the same as those used in the United States; the argument is that Standardization allows users all over the world to access the same services over the Internet.

The question is what impact global technological standards harmonization has on the evolution of national criminal legislation. In terms of unlawful material, Internet users may access information from all over the globe, allowing them to obtain information that is legal in another nation but prohibited on their own. In theory, developments resulting from technical standardization could lead to the harmonization of national laws, in addition to the globalization of technology and services. However, as shown by the negotiations over the First Protocol to the Council of Europe Convention on Cyber crime (the "Convention on Cyber crime"), the principles of national law change much more slowly than technical developments. Although the Internet may not recognize border controls, there are means to restrict access to certain information. In general, the access provider can block particular websites, and the service provider that hosts a website can prohibit access to information for those users based on IP addresses associated with a certain nation ("IP-targeting"). Both methods can be avoided, but they are nonetheless tools that can be used to preserve territorial distinctions in a global network. According to the OpenNet Initiative, around two dozen nations engage in this type of restriction (Zittrain, 2006).

Lessons for Developing Countries

Cyber crime prevention strategies and solutions are major issues and challenges, particularly for underdeveloped nations. A comprehensive anti-cyber crime plan would often

include both technological and legal safeguards. The creation and implementation of these safeguards will take time. Technical safeguards are particularly expensive.

Developing nations must incorporate security measures into the Internet's roll-out from the start because while this may initially raise the cost of Internet services, the long-term benefits of avoiding the costs and damage inflicted by cyber crime are substantial and far outweigh any initial outlay on technical security measures and network safeguards (Michael, Boniface & Olumide, 2014). The dangers connected with lax protective measures may in reality have a greater impact on poorer nations due to their less stringent safeguards and protection. The capacity to safeguard both consumers and businesses is a key necessity not only for traditional organizations but also for online or Internet-based enterprises. Without Internet security, developing nations may face major challenges in growing e-business and participating in online service sectors.

This is because most cyber criminals may commit major computer crimes using cheap or second-hand computer technology expertise is considerably more essential than equipment. The status of computer technology has little impact on whether or not it is used to commit cyber crime. In addition, the usage of specialist software tools may make cyber crime easier. Due to mirroring techniques and peer-to-peer exchange, it is difficult to limit the widespread availability of such devices. Offenders can download software tools designed to locate open ports or break password protection. It is difficult to limit the widespread availability of such devices due to mirroring techniques and peer-to-peer exchange. The final requirement is access to the internet (World Information Society Report 2007).

Although Internet access in most developing countries is more expensive than in developed countries, the number of Internet users in developing countries is rapidly increasing, meaning offenders will generally not subscribe to an Internet service to reduce their chances of being identified, preferring instead services that do not require (verified) registration otherwise referred to as "wardriving". This expression refers to the act of driving about seeking for open wifi networks, as it is commonly called ‘café’ in Nigeria. Public Internet terminals, open (wireless) networks718, hacked networks, and prepaid services without registration restrictions are the most frequent means thieves employ to access the network reasonably anonymously (Ajayi, 2015).

Therefore, to prevent illegal misuse of internet services, third world governments must take deliberate steps to limit unregulated access. The usage of public Internet terminals in Italy and China, for example, necessitates user identification. However, according to International Telecommunication Union, (2006), there are reasons against such criteria for identification despite its advantages to prevent crimes and make law enforcement investigations easier; such laws may stifle the development of the information society and e-commerce. It has been claimed that restricting access to the Internet may infringe human rights.

This was the case with the Nigerian state following the ban of X access. It was also pertinent to note that despite the argument of the infringement of human rights, the ban of X in Nigeria had also created room for more illegal and unrestricted access to the internet, thus providing more frequent means for internet offenders to access the network reasonably anonymously as the majority of the populace were currently using virtual private network (VPN) to access X. It was thus critical for both developed and developing countries to establish technical measures to enhance cyber-security and appropriate cyber crime laws. When compared to the expenses of subsequently grafting safeguards and protection mechanisms onto computer networks, it was likely that early steps adopted from the start would be less expensive. Developing nations had to align their anti-cybercrime policies from the start with international standards.

Nigeria, like the majority of countries, understands the significance of cyber security and is actively participating in the implementation of the Global Cyber Security Agenda, as well as taking real actions to safeguard its cyberspace. However, in his comparative analysis of Nigerian National Cyber Security Policy and Strategy analysis with similar documents of selected countries, across the globe, Oluwafemi & Agada, (2015) submitted that the policy documents are reasonably comprehensive in terms of content. The evaluation based on the harmonized frameworks also showed that the required contents expected to be typically contained in such documents are largely present. unfortunately, certain aspects that appear to be critical to the Nigerian scenario such as an explanation of the current national cyber security state, partnership with internet service providers, the establishment of digital identity frameworks, and the development of a military cyber defense capability were seen to either be utterly absent or only barely implied.

Only recently the Central Bank of Nigeria banned cryptocurrency after the Federal Bureau of Investigation informed the apex bank and the Federal Government that online fraudsters were using it to bring millions of dollars into the economy. Distributed Denial of Service, Credit Card Fraud, Malware, Bad Bots, and e-skimming are some of the other security concerns that are widespread with internet use, particularly in the field of e-commerce. This of course shows a clear lack of synergy or partnership with internet service providers.

Although Agbakwuru, (2021) opined that it was as a result, the National Cyber security Policy and Strategy updated in 2021 to offer the essential framework to effectively combat the changing nature of cyber threats in the country. The National Cyber security Policy and Strategy 2021 equally create a platform that would make it possible to harness the efforts of the private sector, academia, and industry towards progressive economic and national development. It provides the necessary framework needed for technical education, digital skills acquisition, and indigenous technology production, thereby creating job opportunities for youths and supporting resolve to alleviate poverty and boost the economy.

Conclusion and Recommendations

As the volume and sophistication of cyber-attacks grow, given the dominance of ICTs in our daily lives cyber security becomes more important for individuals, families, businesses, and governments. Because cyber-attacks require a loophole or entry point through which the attack can be replicated, all hands must be on deck to effectively combat this threat. Again, we conclude that the cyber security is a continuous process that must be updated on a regular basis. Network defenders must constantly be in the fight to defeat new programs and cyber intruders who develop and exploit new vulnerabilities in computer programs and systems.

In this light the paper recommends that it is vital not only to educate the people involved in the fight against cyber crime but also to draft adequate and effective policy administration and legislation to combat cyber crime, this emphasizes the need for the government security agencies to know that there is a need to keep up with technological and security advancements, as it will always be a losing battle if security professionals are miles behind the cyber criminals. As a sequent of this, Governments should maintain an enormous amount of personal data and records of citizens, as well as confidential government

information, making them frequent targets. Individuals and business entities should observe simple rules, on their part they should ensure proper anti-malware protection on their computer system, encouraged to avoid pirate software, never to share their Identification Number (PIN), bank account, email access code to unknown persons. Finally, there is a need to create cyber-security awareness among the populace.

References

Adeyemi, A (2020) "86% of Nigerian firms fall victim to cybersecurity breaches" https://guardian.ng/

Atherton, M. (2010) Criminals switch attention from cheques and plastic to internet transactions. The Sunday Times of March 10, 2010 9. Aytes, Computer Security and Risky Computing Practices: A Rational Choice Perspectivehttp ://dailyindepen denting .com/2014/0 6/tackling -cyber-security-threats-nigeria/

Ajayi EFG (2015) The Challenges to Enforcement of Cybercrimes Laws and Policy. *International Journal of Information Security and Cybercrime*, 4(2):33-48. Available at: http://www.ijisc.com/year-2015- issue-2-article-4/

Bohn, C & Langheinrich M. Rohs, (2010) Living in a World of Smart Everyday Objects - Social, Economic & Ethical Implications, Journal of Human and Ecological Risk Assessment, Vol. 10, pge 763: www.vs.inf.ethz.ch/res/papers/hera.pdf.

BinaKotiyal, R Goudar, H. (2013) A Cyber Era Approach for Building Awareness in Cyber security for Educational System in India PritiSaxena, IACSIT *International Journal of Information and Education Technology*, Vol. 2, No. 2,

Clark, (2005)"Storage Virtualisation Technologies for Simplifying Data Storage and Management" NS,.

Gercke. M,(2006)The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International, , page 142.

Gercke M, (2012) "Understanding cybercrime: Phenomena, challenges and legal response"www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Goodman, S (2011) The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 3, available at: http://media.hoover.org/documents/0817999825_1.pdf

International Telecommunication Union (2008) "World Information Society Report 2007", Geneva, available at: www.itu.int/wisr/

International Telecommunication Union, (2006) ITU Survey On Anti-Spam Legislation Worldwide: Itu Survey On Anti-Spam Laws Worldwide

International Telecommunications Commission (2011) "Making the Online World Safer" http://www.itu.int/net/itunews/issues/2011/05/38.aspx

Iyengar, R, (2020) "Twitter accounts of Joe Biden, Barack Obama, Elon Musk, Bill Gates, and others apparently hacked". CNN Business. Archived from the original on July 16, 2020.

Keizer, (2005) Dutch Botnet Suspects Ran 1.5 Million Machines, TechWeb, 21.10.2005, available at:www.techweb.com/wire/172303160

MichaelA.,Boniface., A. and Olumide, A. (2014) *Mitigating Cybercrime and Online Social Networks Threats in Nigeria*, Proceedings of the World Congress on Engineering and Computer Science Adu Michael Kz, vol. Vol I WCECS 2014, 22–24.

Oluwafemi O & Agada D. O, (2015) National Cyber Security Policy and Strategy of Nigeria: *A Qualitative Analysis International Journal of Cyber Criminology* (IJCC) ISSN: 0973-5089 - January – June 2015. Vol. 9 (1): 120–143. DOI: 10.5281/zenodo.22390

Olasanmi, O. O (2010). Computer Crimes and Counter Measures in the Nigerian Banking Sector. *Journal of Internet Banking & Commerce,* 15(1), 1-10 (http://www.arraydev.com/commerce/jibc/)

Schatz D, Bashroush. R & Wall J, (2017) "Towards a More RepresentativeDefinition of Cyber Security Cyber Security," *Journal of Digital Forensics, Security and Law: V*ol. 12: No. 2 , Article 8. DOI: https://doi.org/10.15394/jdfsl.2017.1476

Schjolberg. T, (2005) Harmonizing National Legal Approaches on Cybercrime,, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf; https://www.vanguardngr.com/2021/02/buhari-seeks-overhaul-of-national-strategy-on-cyber-security-2/

Ravi S, (2012) Study of Latest Emerging Trends on Cyber Security and its challenges to Society. *International Journal of Scientific & Engineering Research, Vol 3, Issue 6,* -1 ISSN 2229-5518 IJSER

World Economy Forum (2020) Global Risk Basement Report, The https://www.weforum.org/reports/the-global-risks-report-2020

Zittrain, J. (2006) A History of Online Gatekeeping Harvard Journal of Law & Technology Volume 19, Number 2 Spring 2006