Journal of Central and Eastern European African Studies

Here there be Dragons: Evolution, Potentials and Mitigation Opportunities of Cybercrime in Nigeria[1]

A Review, Analysis, and Evaluation

Attila Máté Kovács[2]

Abstract:

The world is becoming increasingly interconnected due to advancements in technology and the adoption of the internet. The once widely used traditional forms of communication such as parcels have become unpopular. The development of computers and the internet has become the primary mode of communication. Internet is now widely used across businesses, government departments, and individual mobile connectivity. However, the increased internet use has posed modern threats attributed to cybercrime. Nigeria is experiencing growth in population and internet connectivity, with an internet penetration of 33.6%. With an estimated population of just over 205 million people, the impacts of cybercrime will continue to increase. Nigeria is now regarded as the cradle of cybercrime activities in sub-Saharan Africa. Cybercrime is estimated to cost the economy of Nigeria $649 million annually. Besides, cybercrime activities have other impacts, such as impersonation and plagiarism. Due to the scale of these impacts, it is imperative that an adequate capacity to handle emerging issues in cybercrime be developed. The study investigated cybercrime preparedness in Nigeria. Research findings indicate that Nigeria has inadequate legal and educational preparedness to help mitigate the rising incidences of cybercrime in the country. The country has only one cybercrime act passed in 2015 and five universities that offer cybercrime-specific courses.

Keywords:

Cybercrime, cyber threats, education, information technology, policy, Nigeria.

[1] DOI: https://doi.org/10.59569/jceeas.2022.2.1.55

[2] PhD-student at Doctoral School for Safety and Security Sciences, University of Óbuda; ORCID: 0000-0001-5088-5749; kovacs.attilamate@uni-obuda.hu.

1. Introduction

The world is facing increasing globalization and the adoption of technology across all sectors of the economy. It is now virtually impossible to find traditional forms of communication, with many people, businesses, educational entities, and not-for-profit organizations adopting technology. As a result, the world has increasingly become a global village. The challenges attributed to communication across borders in the 90s have been overcome, making contact across regional boundaries a near reality. However, an attempt to solve communication challenges has led to one of the most significant modern challenges. The adoption of technology has led to unprecedented concerns about the threats of technology to individual, organizational, and government privacy.

The title also refers to the unknown and sometimes vague perceptions about cybercrime. Medieval mapmakers supposedly inscribed the phrase “Here Be Dragons” on maps showing unknown regions of the world (Van Duzer, 2013). Today, one of the most significant challenges that are now facing the world as a whole is the threat of privacy attributed to cybercrime. Although Western countries have made massive steps towards adopting measures to detect and prevent cybercrime, African countries still lag.

Almost all African countries do not have elaborate technological frameworks to handle the threats posed by cybercrime. The dangers posed by cybercrime were estimated to cost African countries an average of $3.7 billion in 2017 alone (Kshetri, 2019). The author notes that Nigeria lost an estimated $649 million to cybercrime activities in the same year alone. The financial implications of cybercrimes in Nigeria will become more complex in the coming decade. As Nnanwube, Ani, and Ojakorotu (2019) notes, cybercrimes in the country will keep evolving with new dimensions taking shape as the perpetrators encounter new systems. Besides, the growing adoption of technology across the different sectors of the economy and a rapidly growing population will continue to add to its complexity. Given the significant impact of cybercrime in Nigeria, this paper reviews, analyses, and evaluates cybercrimes in the country to make recommendations.

2. Literature review

The concept of cybersecurity has undergone a massive transformation over the past two decades (Garba and Bade, 2021). Initial cybersecurity efforts focused on protecting the user’s computers and operating systems. However, cybersecurity has emerged as a transition of the adoption of computers and the internet. The term cybersecurity encompasses the methodologies of protecting entity assets by identifying threats that have the potential to compromise important information stored within the organization's computer systems (Alese et al., 2014). The authors note that cybersecurity encompasses identifying, protecting, and responding to threats. Due to the significant adoption and penetration of mobile telecommunication, the impacts of cybersecurity crimes have become a significant source of

concern in Nigeria. The country is facing unprecedented challenges in combating cybercrime. Cybersecurity challenges facing the country can be traced as far as the 1990s.

The growth in mobile interconnectivity and increased internet penetration has coincided with increasing global cybersecurity concerns. Research shows an increase in the cost associated with cybercrimes. The annual cost of cybercrime is estimated at over $1 trillion (Ajayi, 2016). In Africa alone, cybercrime costs are estimated at just over $375 billion. In a country with a rapidly growing population, the impacts of cybercrime in Nigeria are bound to have significant economic implications for the country. The government is reportedly losing over $649 million annually to cybercrime-related activities. The losses have been linked to massive internet penetration buoyed by the increasing number of mobile subscribers. Nigeria is now regarded as the tenth-largest user of the internet, which exacerbates the threats associated with cybercrime. The number of internet users in Nigeria has been expanding continually since 2012. In 2009, the country had about 44 million internet users (Doyon-Martin, 2015). In contrast to cellphone adoption, the g had about 112 million, relative to the country's population estimated at 177 million. The ratio of the number of cellphones to the population indicates an impressive number of subscribers, which ranks above the top 20 in the world.

As a developing country with the highest population density in Sub-Saharan Africa, Nigeria is among Africa's top sources of cybercrime. Besides, developing countries are considered the leading grounds for hacking (Kshetri, 2010). According to the authors, 92% of global trojans have origins in developing countries. In 2002, the country was ranked the top sixth country in the number of attacks per 10,000 internet users. One of the major contributors to increasing incidences of cyber-attacks in Nigeria is unemployment rates. Nigeria is experiencing an increasing number of techno-savvy youths, often referred to as yahoo boys. This group of individuals were born and educated in the technological era and possessed potent specialized skills (Ebenezer, Paula, and Allo, 2016). Unfortunately, upon acquiring education and skills, there are very few employment opportunities. The country recorded unemployment rate of 23% in 2018, which renders many skilled youths into cybercrime activities. The other factors that have been blamed on the rising rates of cybercrimes in Nigeria are desperation to make wealth, inadequate cybercrime laws, few forensics experts, urbanization, and negative role models.

In a bit to save its face, Nigeria is now directing its efforts toward combating cybercrimes and their impacts (Odumesi, 2014). Most of the steps to fight cybercrime in the country are towards the sources and channels through which the crime is perpetuated. Consequently, the government has identified several common cybercrimes. The most prevalent types of cybercrimes identified and targeted include fraud-identity (Ogunleye, Ojedokun, and Aderinto, 2019). Online identity fraud is the most common form of cybercrime in Nigeria that is perpetuated for financial gains (Iorliam, 2019). The vice is committed through cloning websites that act as baits to unsuspecting individuals, prompting them to share their personal information. The other common forms of cybercrimes in Nigeria are hacking, cyberterrorism

(Besenyő, Sinkó, 2021), web jacking, cyberstalking, ransomware, and software piracy. The increased incidences of cybercrime have led to suffering across different sectors of the Nigerian economy.

The impacts of cybercrime in Nigeria are widespread across the different sectors of the country's economy. Although confidentiality is so important for financial and healthcare information, this is hard to guarantee in Nigeria (Iorliam, 2019). When the accuracy and trustworthiness of information are secured, it increases integrity. However, confidentiality and integrity of data in Nigeria are largely compromised. According to the author, the lack of privacy and privacy of information in the country can be attributed to factors such as network design, communication channels, software, that are exploited by cybercriminals for financial gains or victimization purposes. The FinTech sector, for instance, has expressed the need to push "suspicious transactions" and investment in cybercrime (Gaillard, 2021). Besides the FinTech sector, the other sectors affected by cybercrime in Nigeria are the social media, education sector, and the e-commerce sector.

The most rampant forms of cybercrimes in Nigeria occur within the banking sector. Although the banking sector has continued to improve its banking security measures, the fraudsters have equally improved their attack skills (Omodunbi et al., 2016). The author notes that several lucrative attacks aimed at the banking sector have been perpetuated with success. The majority of these attacks are undertaken with the goal of obtaining the funds from the bank accounts of the victims without their express authority. However, some bank attacks have been undertaken to destroy the reputation of the affected banks. Some of the leading cyberattacks that have affected the banking sector in Nigeria can be categorized as phishing, bank verification number (BVN) scams, the theft of bank cards, and attacks that target vulnerable banks accounts. Despite different types of banks attacks, what is expected in most of such attacks is financial gains. Fraudsters that target the banking sector employ various strategies such as cloned websites and keyloggers in cybercafes to steal important information that is later used to perpetrate banking frauds.

Besides banking fraud, the development and increased use of social media have increased cybercrimes that target social media users. Omodunbi et al. (2016) outline that the use of social media in Nigeria has gained pace across different sectors of the economy. The continued increase and use of social media expose people to hackers and possible loss of personal information (Agara et al., 2021). Omodunbi et al. (2016) note that the most prominent social media sites in Nigeria that are avenues for cybercrime attacks are Twitter, Facebook, LinkedIn, and Instagram. According to the authors, these social media platforms have been the target grounds for cyber-attacks. The ability of social media to remove the barriers such as social, economic, and geographic barriers make it a fertile ground for the perpetuation of crime. Some of the renowned cyber scans that have been carried through social media platforms include the Nigerian-Prince scam and the charity funds fraud. Besides, other common social

media cybercrimes that have been reported are blackmailing, harassment, cyber-stalking, and social-hijacking.

Moreover, cybercrime in the education sector is another rising form of cyberspace attack in Nigeria (Omodunbi et al., 2016). The author notes that the education sector in the country has experienced massive cyberattacks that originate from students in higher institutions of learning. Many of the cases that result from students in polytechnics and universities occur because of inefficient management and inadequate resources. The authors point out that cyber-attacks in the education sector have resulted in massive financial, intellectual property, and social losses. In addition to the education sector, e-commerce faces massive impacts of cyberspace attacks in the country. Nigeria enjoys a vibrant economy with a booming business sector that is rapidly adopting technology. However, cyberspace attacks have been recognized as one of the country's leading threats to e-commerce providers. According to the author, e-commerce entails the use of technological devices, applications, and the internet in the purchase, sale, and marketing of services and goods. Since e-commerce employs technological platforms, it is prone to attacks such as hacking, phishing, impersonation, and scams. Despite growth in crimes in e-commerce, the author notes that fewer reports are made, with entities and individuals preferring to safeguard their integrity. Some affected entities and individuals fear making reports because of fear of losing business that would result from negative publicity. Besides, as technology continues to be integrated across Nigeria, the other sectors that continue to experience growth in threats are healthcare, public service, agriculture, law enforcement and crime control, trade and commerce, media and communication, and politics and governance (Nwankwo and Ukaoha, 2019).

The impacts of crimes attributed to cyberspace are enormous and amount to about 0.08% of the GDP of Nigeria (Nwankwo and Ukaoha, 2019). In a country that is facing serious and growing unemployment rates, the impacts of cybercrime will continue to be felt across all the sectors of the economy. Besides, the rapidly growing population, increasing internet connectivity, a growing mobile base, and increased technology integration in all sectors, cybercrime continues to be a major source of concern.

Legislation itself is a key area. When it comes to finding ways to reduce different types of cybercrime, politicians, the general public, security professionals, and other academics should look to the research conducted by cybercrime scholars as the primary source of knowledge. Regrettably, there is a dearth of evidence-based research that examine the efficacy of legislation regarding cybercrime. In the article titled "Enhancing the Effectiveness of Cybercrime Prevention through Policy Monitoring" (Dupont, 2019), the author argues that countries all over the world have spent massive sums of money to invest in cybersecurity, but that these countries have not spent the resources to develop tools to assess the effectiveness of government interventions in reducing cybercrime.

According to Dupont, policy monitoring would result in a more robust knowledge base regarding the efficacy of cybercrime policies because it would lead to the systematic collection

of data, rigorous evaluations, and widespread dissemination of the evaluation results. This is why policy monitoring would lead to a more robust knowledge base regarding the effectiveness of cybercrime policies. In his examination of eighteen different policy surveillance platforms, he describes the most important aspects of each one and explains how each one might be utilized in the fight against cybercrime. He contends that the development of a cybercrime preventive surveillance tool has to be regarded as a priority in light of the negative effects that are associated with cybercrime. Dupont writes as follows: 'It is now up to cyber-criminologists to determine the relevance of this framework, its feasibility, and the collaborative resources that would be need to translate it into reality.'

3. Methodology

The historical method of research and analysis was employed in this research article. The main goal of this research was to perform a critical analysis of the cybersecurity measures that have been enforced in Nigeria. The research began with a comprehensive review of the general published literature on cybersecurity in the country. Besides, additional published materials from other jurisdictions were considered in the article. Once the literature review was completed, a systematic and in-depth review of the existing policies that govern cybercrime in Nigeria were examined. In order to ensure adequate and appropriate published literature was obtained, several keywords were employed. The keywords that were employed in the research were cybercrime, cyber threats, education, information technology, policy, and Nigeria. These keywords yielded over 8,500 published articles. However, not all the published content was relevant to the topic under the study.

In order to narrow down and ensure that only appropriate research papers were examined, inclusion and exclusion criteria were established. The inclusion criteria that were established was that the publications should have been dated 2016 or earlier. Besides, only credible research articles were chosen for the research article. Moreover, additional research articles that analyzed policies in the U.S were considered for the purposes of enriching the evaluation. Since the report analyzes the cybercrime policies in Nigeria, published government policies were also considered. The government publications provided primary sources for counterchecking with information obtained from the published research articles.

The study data collected through the documentation of the secondary information was later analyzed. Some other sources of information from which the basis of the article was developed included newspapers, videos, photographs, and other sound recordings. These additional sources were analyzed for the contemporary development of the research paper. All the primary and secondary data collected was then collated, and findings were represented in the form of themes that were identified. An in-depth analysis was then undertaken, followed by an evaluation that considered other jurisdictions that have made decisive steps in cybercrime prevention. Finally, the article draws on the study findings to conclude the status of cybercrime in Nigeria.

4. Typology and prevention

Today's major cybercrime trends and risks include: (1) ransomware; (2) other malware threats; (3) data breaches and network assaults; (4) phishing; (5) spearphishing (targeting specific individuals in order to distribute malware or collect sensitive information); and (6) attacks against key infrastructure.

Phishing is one of the most common types of cybercrime and involves perpetrating computer fraud in order to steal sensitive information from an unsuspecting victim. This information can include credit card numbers, usernames and passwords for online banking platforms, personal information about the victim, and other sensitive information. "[i]ndividual cybercrime victimization is much greater than for "traditional" criminal types," states the Comprehensive Study on Cybercrime that was conducted by the United Nations Office on Drugs and Crime (UNODC). The percentage of the internet population that falls victim to crimes such as online credit card fraud, identity theft, responding to a phishing effort, or suffering illegal access to an email account ranges from 1 to 17 percent (UNODC, 2013).

These types of changes create new issues both at home and abroad, such as indiscriminately damaging targets, increasing existing low levels of reporting to authorities, and legislative challenges, necessitating new policy solutions. Other trends that should ideally continue to be considered by law enforcement and policymakers involved in the fight against cybercrime include the growing links between cybercrime and malevolent state activity; IoT/future cities and smart meters; cloud security; emerging technologies; third party vendor risks and supply chain attacks; widespread public and commercial availability of tools and techniques as well as "Darknet" concerns; and poor security cultures.

5. Cybercrime overview in Nigeria – social and legal context

The Nigerian government has prioritized the prevention of cybercrime for a number of years. In Nigeria, multiple government agencies, including the Economic and Financial Crimes Commission (EFCC), the Independent Corrupt Practices and Other Related Offenses Commission (ICPC), the State Security Services (SSS), and the Nigerian Police, all play significant roles in the fight against the rising tide of cybercrime. In particular, the Economic and Financial Crimes Commission (EFCC) has been conducting investigations into many aspects of cybercrime related to fraud. Despite the fact that the Evidence Act was amended in 2011 to permit the admission of electronic evidence, until 2015, effective criminal justice procedures were hampered by the absence of a legal framework for cybercrime. This was the case despite the fact that the Evidence Act was revised in 2011 to allow for the admission of electronic evidence.

The Nigerian government gave its approval to the National Cybersecurity Policy and Strategy in February of 2015. This policy and strategy were developed by the Inter-Ministerial Committee and is handled by the Office of the National Security Adviser.

It is predicated on the idea that threats to information and communication technology pose a risk to the national security of Nigeria and have an impact on the "economic, political, and social fabric" of the nation. The most significant problems that have been identified are cybercrime, cyberespionage, cyberconflict, cyberterrorism, and the abuse and exploitation of children who use the internet. Its mission is to mitigate cyber security threats in a manner that is consistent with the overriding objective of ensuring national security. The implementation of this policy has thus far resulted in significant benefits for boosting Nigeria's cyber resilience.

Legislation regarding cybercrime and electronic evidence is required to fulfill a variety of conditions, including the following:

- It is imperative that it be sufficiently (technologically) neutral in order to handle the ongoing evolution of both technology and crime; otherwise, there is a chance that it will become obsolete before it ever goes into operation.
- For example, to fulfill the dual criminality criteria, it must be sufficiently harmonized with the laws of other nations, or at the very least consistent with those laws, in order to permit international collaboration.

The significant commitment of the member states of the African Union to the establishment of a secure and dependable foundation for the information society is demonstrated by this treaty. It involves a wide range of different measures, including electronic transactions, the protection of personal data, the prevention of cybercrime, and cybersecurity.

The current study makes reference to the Budapest Convention on Cyber Crime because of its widespread applicability as well as the fact that it is a relatively new convention that has not yet been validated in actual practice (Council of Europe, 2001). This Convention, which is being implemented throughout Africa at a growing rate, focuses on cybercrime and electronic evidence in addition to international cooperation.

The Nigerian officials who are crafting the country's cybercrime law may look to a range of sources for guidance. Malabo, in the country of Equatorial Guinea, was the location where the African Union Convention on Cyber Security and Personal Data Protection was ratified in June of 2014.

6. Specific results and underlying details

Analyzing the published literature, primary sources, and other relevant cybercrime publications revealed several themes. The study identified two main themes: the country’s regulatory framework, education, and readiness. The most dominant theme placed is the cybercrime regulatory framework in Nigeria. The government first created The Cybercrime Advisory Council in 2016, whose responsibility was to formulate modalities for implementing

the Cybercrime Act of 2015. Table 1 summarizes the regulation that governs cybercrimes in Nigeria and the types of crimes that the regulation covers.

Cybercrime Act	Types of Crimes Governed by the Laws
Cybercrimes Act of 2015	-Crime against critical national infrastructure. -Unauthorized access to protected systems. -Illegal registration of cybercafes. -System interference. -Interception of electronic messages, emails, and electronic money transfers. -Willful misdirection of electronic messages. -Unlawful interceptions. -Computer-related forgery. -Computer-related fraud, electronic cards fraud. -Identity theft, impersonation, tampering with computer sources. -Cyberstalking, cybersquatting, cyberterrorism, breach of privacy and confidentiality. -Phishing, spamming, spreading of computer viruses. -Publishing false electronic signatures and certificates.

Table 1: Laws that Have Been Passed in Response to Cybercrimes in Nigeria

In addition to the regulatory framework, the institutional framework in terms of capacity building was analyzed. Nigeria has a total of 160 universities located in different states, offering various courses. Table 2 below summarizes the universities in Nigeria, including their zoning and the nature of ownership. While narrowing down the focus of the study, only the accredited universities were analyzed, and the results were presented. As a result, the study found that only sixteen accredited universities offer cybercrime-related education in the entire country (Samphina Academy, 2019). Table 2 summarizes the findings of the institutional analysis of cybersecurity in Nigeria.

Location/Ownership	Federal	State	Private	Total
North Central	6	5	7	**18**
North East	6	7	2	**15**
North West	9	7	1	**17**
South East	5	6	13	**24**
South-South	6	9	13	**28**
South West	8	12	38	**58**
Total	**40**	**46**	**74**	**160**

Table 2: The Location and the Number of Universities in Nigeria

University Name	Year the University was Established
American University of Nigeria, Yola	2004
Oyo State Technical University, Ogbomoso	2012
Bayero University	1975
Federal University of Technology, Akure	2011
Federal University of Technology, Owerri	1980

Table 3: The Number of Educational Institutions that Offer Cybercrime Education

7. Discussion

About a billion people in Africa will have access to the internet by 2022 (Kshetri, 2019). However, experts point out that significant cybercrime impacts that attract attention occur once an internet penetration threshold of 10-15% is achieved. In Nigeria, the current penetration threshold stands at 33.6%, boasting 108 million users (Statista, 2017). The authors note that industry projections indicate that internet penetration will increase and reach about 143.26 million people in Nigeria by 2026. Despite the increasing threats of cybercrimes due to growing internet penetration, the findings show that Nigeria is still lagging in capacity development.

Nigeria has a limited legal framework to deal with the rapidly changing trends in cybercrimes. As cybercrimes continually evolve, similarly, the legal, regulatory framework must be proactive. Although table 1 indicates that Nigeria has some legal framework governing cybercrime, the laws were enacted in 2015. These legislations seemed reactive in the first place since the country existed without cybercrime laws up to 2015, when the Cybercrime Act of 2015 was passed. Comparatively, developed jurisdictions such as the United States of America have passed different legislation about internet crimes. The US, which has different states similar to Nigeria, has passed federal cybercrime laws and 51 other related

laws across its 51 states (Hill and Marion, 2016). For example, as businesses moved online, the country developed the Digital Millennium Copyright Act of 1998. The act extends the long-standing copyright act that seeks to protect copyright owners against piracy. Thus, it can be argued that whereas cybercrimes evolve continuously, Nigeria exhibits a reactionary and static approach towards cybercrime and emerging developments.

Although Nigeria has established laws governing cybercrime, there is a lack of specific rules that handle major cybercrimes in the modern era. The United States became the first country to enact laws that criminalized cybercrimes (Hosani et al., 2019). The early adoption of rules governing cybercrime in the U.S could be attributed to the country's early adoption and use of the internet. Although Nigeria is a relatively young democracy, the growing population, increasing internet penetration, and concerns of growing cybercrimes must be reflected in its cybercrime law. However, the Cybercrime Act of 2015 fails to capture these growing concerns as the internet penetration in Nigeria grows, the incidences of cyberbullying are similarly increasing in the country (Adediran, 2020). For instance, the FBI ranks the country 16th in the world regarding the number of cybercrime cases. Besides, there are growing concerns that the Cybercrime Act of 2015 may not be adequate for dealing with emerging cybercrime cases (ISSAfrica.org, 2020). Moreover, despite the existing laws, many entities continue to experience increased incidences of cyber-attacks. Although some cases may be attributed to a lack of adequate cybercrime preparedness, forms of cybercrimes such as disinformation and impersonation are directly dealt with through existing legal frameworks.

Besides an inadequate legal framework, Nigeria lacks adequate education dealing with cybercrime. As indicated in the research findings, only five accredited universities provide education on cybercrimes. Despite a rapidly growing population and evolving cybercrime network, the education center is not expanding appropriately. Although the country has over sixty universities, most of these institutions do not provide education that directly addresses cybercrime. This means that fewer professionals that provide cybercrimes expertise, relative to other fields, graduate into the job market annually. Numerous studies have indicated the significant role that education plays in preventing cybercrime. Back and LaPrade (2019) notes that cybercrime technology that can fight cyberspace crimes continues to be developed. However, the authors point out that this may not be adequate because it cannot impact human behaviors. The authors note that we cannot rely only on technology such as software to halt cybercrimes. Humans will continue to be vulnerable, with other forms of cybercrime such as phishing, impersonation, and bullying inadequately solved by emerging technologies. Technological and cybercrime education remains the best alternative to augment technical solutions towards cybercrime.

Whereas education remains a critical step in fighting cybercrime, Nigeria lags in infrastructural development. The lack of increased investment in cybercrime courses coupled with increasing growth in incidences of cybercrime presents a bleak future for internet users in Nigeria. In terms of increasing the number of colleges that offer cyber security-specific courses, capacity building is one of the critical steps in the fight against cybercrime. For

example, In the United States, California, with about 40 million people, has over 25 schools that offer 54 cybersecurity courses (Cybersecurity Guide, 2021). Although other factors such as economic potential and the presence of skilled workforce play a role, comparatively, Nigeria needs to invest more in cybersecurity courses. The economy of California dwarfs that of Nigeria, which has allowed it to have the capacity to support in cybercrime courses. However, Nigeria could improve its ability to fight cybercrime if it increased the number of studies in universities relative to its population. In a country with over 100 million people and 60 universities, having only five accredited cybercrime-specific courses indicates underinvestment.

8. Conclusion

The adoption of computers and electronic communication is rapidly evolving. Many people are now connected to the web more than a decade ago, with increasing mobile connectivity bound to increase the number of internet users. In developing countries in sub-Saharan Africa, internet penetration continues to expand. More and more people are now adopting mobile banking, electronic commerce, and social media communication. While these innovations improve communication and efficiency of conducting business, it comes with unprecedented challenges of increased cybercrimes (Besenyő, Gulyás, 2021). Countries in sub-Saharan Africa, such as Nigeria, continue to struggle with rising incidences of cybercrimes. Whereas developed countries such as the United States boast adequate counter-cybercrime measures, Nigeria lags in all aspects of its responses. The government is facing a growing population and increasing internet penetration, yet little has been done in capacity building to cope with cybercrime threats growing. The country must invest more in its legal framework and education that offers cybercrime courses. As the world moves into the next stage of technological advancement, Nigeria must adopt a proactive approach to enhance its capacity to respond to cybercrime activities.

Conflict of Interest

The author hereby declares that no competing financial interest exists for this manuscript.

Notes on Contributor

Attila Máté Kovács (Óbuda University Doctoral School on Safety and Security Sciences; Cognizant [CEHv11 Certified Ethical Hacker; Certified Chief Information Security Officer and ISO27000 auditor]). After earning a post-graduate degree in Energy Economics from the Regional Centre for Energy Policy Research, Budapest Corvinus University for a thesis on Electricity Capacity Mechanisms, he also deepened his knowledge in two proficiency fields of his interests, Artificial Intelligence and Machine Learning, at Kürt Academy and Stanford. At the start of his career, he worked as a strategy consultant at Roland Berger Strategy Consultants and Accenture and later also at Cyber Services Plc in international information security Research & Development projects. Before joining Cognizant in 2021 in an Information Security Management position, he worked at the air navigation service

provider Hungarocontrol, personally contributing to remote tower and unmanned aerial vehicle development and regulatory initiatives.

Bibliography

Adediran, A. O. (2020) 'Cyberbullying in Nigeria: Examining the Adequacy of Legal Responses', *International Journal for the Semiotics of Law - Revue Internationale de Sémiotique Juridique*, 34(4), pp. 965-984.

Agara, E. P., Ojong, F. E., Emeka, J. O., Agba, A. M. O., Akintola, A. I. and Ogunsola, O. V. (2021) 'Social Media Platforms: Exposing Students to Cybercrimes', *ARRUS Journal of Social Sciences and Humanities*, 1(1), pp. 44-54.

Ajayi, E. F. G. (2016) 'Challenges to Enforcement of Cyber-crimes Laws and Policy', *Journal of Internet and Information Systems*, 6(1), pp. 1-12.

Alese, B. K., Thompson, A. F., Owa, K. V., Iyare, O. and Adebayo, O. T. (2014) 'Analyzing Issues of Cyber Threats in Nigeria' in Ao, S. I., Gelman, L., Hukins D. W. L., Hunter, A. and Korsunsky, A. M. (eds) *Proceedings of the World Congress on Engineering*. London: World Congress on Engineering, pp. 1-7.

Back, S. and LaPrade, J. (2019) 'The Future of Cybercrime Prevention Strategies: Human Factors and a Holistic Approach to Cyber Intelligence', *The International Journal of Cybersecurity Intelligence and Cybercrime*, 2(2), pp. 4.

Besenyő, J. and Gulyás A. (2021) 'The Effect of the Dark Web on the Security', *Journal of Security and Sustainability Issues*, 11, 103-121.

Besenyő, J. and Sinkó, G. (2021) 'The Social Media Use of African Terrorist Organizations: A Comparative Study of Al-Qaeda in the Islamic Maghreb, Al-Shabaab and Boko Haram', *Insights into Regional Development*, 3(3), pp. 66-78.

Council of Europe (2001) *Convention on Cybercrime (ETS No. 185)*. [online] Available at https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 (Accessed: 8 December 2021).

Cybersecurity Guide (2021) *Cybersecurity Degree Programs in California | 2021 List*. [online] Available at https://cybersecurityguide.org/states/california/ (Accessed: 13 December 2021).

Doyon-Martin, J. (2015) 'Cybercrime in West Africa as a Result of Transboundary E-Waste', *Journal of Applied Security Research*, 10(2), pp. 207-220.

Dupont, B. (2019) 'Enhancing the Effectiveness of Cybercrime Prevention Through Policy Monitoring, *Journal of Crime and Justice*, 42(5), pp. 500-515.

Ebenezer, A. J., Paula, A. M. and Allo, T. (2016) 'Risk and Investment Decision Making in the Technological Age: A Dialysis of Cyber Fraud Complication in Nigeria', *International Journal of Cyber Criminology*, 10(1), pp. 62-78.

Gaillard, A. (2021) 'Cybersecurity Challenges and Governance Issues in the Cyberspace "When Stronger Passwords Are Not Enough: Governing Cyberspace in Contemporary African Nations" Case Study: Can South Africa and Nigeria Secure Cyberspace without a Lock?', *SSRN Electronic Journal*. [online] Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3877526 (Accessed: 13 December 2021).

Garba, A. and Bade, A. (2021) 'The Current State of Cybersecurity Readiness in Nigeria Organizations', *International Journal of Multidisciplinary and Current Educational Research*, 3(1), pp. 154-162.

Hill, J. B. and Marion, N. E. (2016) *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century*. Santa Barbara: Praeger.

Hosani, H. A., Yousef, M., Shouq, S. A., Iqbal, F. and Mouheb, D. (2019) 'A Comparative Analysis of Cyberbullying and Cyberstalking Laws in the UAE, US, UK and Canada' in *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA),* pp. 1-7. DOI: 10.1109/AICCSA47632.2019.9035368.

Iorliam, A. (2019) *Cybersecurity in Nigeria: A Case Study of Surveillance and Prevention of Digital Crime*. Cham: Springer International Publishing.

ISSAfrica.org (2020) *Cybercrime in Nigeria Demands Public-Private Action*. ISS Africa. [online] Available at https://issafrica.org/iss-today/cybercrime-in-nigeria-demands-public-private-action (Accessed: 12 December 2021).

Kshetri, N. (2010) 'Diffusion and Effects of Cyber-Crime in Developing Economies', *Third World Quarterly*, 31(7), pp. 1057-1079.

Kshetri, N. (2019) 'Cybercrime and Cybersecurity in Africa', *Journal of Global Information Technology Management*, 22(2), pp. 77-81.

Nnanwube, E. F., Ani, K. J. and Ojakorotu, V. (2019) 'Emerging Issues around Cyber Crimes in Nigeria', *Ubuntu: Journal of Conflict Transformation*, 1(1), pp. 55-71.

Nwankwo, W. and Ukaoha, K. C. (2019) 'Socio-Technical Perspectives on Cybersecurity: Nigeria's Cybercrime Legislation in Review', *International Journal of Scientific & Technology Research*, 8(10), pp. 47-58.

Odumesi, J. O. (2014) 'A Socio-Technological Analysis of Cybercrime and Cyber Security in Nigeria', *International Journal of Sociology and Anthropology*, 6(3), pp. 116-125.

Ogunleye, Y. O., Ojedokun, U. A. and Aderinto, A. A. (2019) 'Pathways and Motivations for Cyber Fraud Involvement among Female Undergraduates of Selected Universities in South-West Nigeria', *International Journal of Cyber Criminology*, 13(2), pp. 389-325.

Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M. and Esan, A. O. (2016) 'Cybercrimes in Nigeria: Analysis, Detection and Prevention', *Journal of Engineering and Technology*, 1(1), pp. 37-41.

Samphina Academy (2019) *List of Nigerian Universities Offering Cyber Security*. Samphina Academy. [online] Available at https://samphina.com.ng/complete-list-universities-offering-cyber-security-nigeria/#Al-Hikmah_University_Illorin_AHU (Accessed: 10 December 2021).

Statista (2017) *Nigeria: Number of internet users 2023 | Statistics*. [online] Available at https://www.statista.com/statistics/183849/internet-users-nigeria/ (Accessed: 12 December 2021).

UNODC (2013) *Comprehensive Study on Cybercrime*. [online] Available at https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (Accessed: 12 December 2021).

Van Duzer, C. (2013) *Sea Monsters on Medieval and Renaissance Maps*. British Library Publishing.