

Old Dominion University

ODU Digital Commons

Cybersecurity Undergraduate Research

2023 Spring Cybersecurity Undergraduate
Research Projects

Cybersecurity Workforce Development in Nigeria: Transforming the Cybercrime Gangs into Cybersecurity Specialists

Olohi Favor Anteyi
Old Dominion University

Follow this and additional works at: <https://digitalcommons.odu.edu/covacci-undergraduateresearch>



Part of the [African Studies Commons](#), and the [Information Security Commons](#)

Anteyi, Olohi Favor, "Cybersecurity Workforce Development in Nigeria: Transforming the Cybercrime Gangs into Cybersecurity Specialists" (2023). *Cybersecurity Undergraduate Research*. 6.
<https://digitalcommons.odu.edu/covacci-undergraduateresearch/2023spring/projects/6>

This Paper is brought to you for free and open access by the Undergraduate Student Events at ODU Digital Commons. It has been accepted for inclusion in Cybersecurity Undergraduate Research by an authorized administrator of ODU Digital Commons. For more information, please contact digitalcommons@odu.edu.

Cybersecurity Workforce Development in Nigeria

Transforming the Cybercrime Gangs into Cybersecurity Specialists

Olohi Anteyi

Cybersecurity Major

Old Dominion University (Expected Graduation Spring 2024)

April 2023

Abstract: This paper addresses the issue of cybercrime in Nigeria and the possibility of creating a cybersecurity workforce development program for cyber criminals to develop their skills for the cybersecurity profession, which may facilitate Nigeria's economic development.

Tables of Contents

- I. Introduction
- II. Background Information
 - a. The State of Cybercrime in Nigeria
 - b. The Current Nigerian Cybercrime Trends
- III. Transition From Cybercrime to Cybersecurity Workforce
 - a. Government Engagement and Funded Cybersecurity Programs
 - b. Government Diversity Recruitment Efforts
- IV. Conclusion

I. Introduction

The Internet is one of the world's biggest achievements. It has provided technological benefits that improved globally the information accessibility among various institutions, but the Internet also introduced novel risks that threaten the livelihood of many individuals and disrupt organizations' operations.¹ This issue plays a larger role in Nigeria, where the developing economy is more prone to the effects of cybercrime. Unfortunately, such environment is rife with banking fraud, vulnerability exploitation, and the quest for wealth for personal or political gain.²

The factors of nepotism, economic struggles, and tribalism this has created unwarranted time for people, specifically youths, to dabble in the world of cybercrime or "419", a term Nigerians have coined for cyber-criminal activities. The government's ongoing efforts failed to develop a resilient economy, especially in Information Technology (IT) and other emerging technology sectors, where people could have found stable and professional work. As a result, many unemployed Nigerians are engaging in cybercrime.

Nigeria faces a rising systemic unemployment crisis with about 20 million unemployed Nigerians, with another 2 million new college graduates on the verge of being largely unemployed.³ Nigeria's reputation has suffered because of cybercrime, both domestically and globally. For decades, Nigeria has been ranked as one of the top ten countries worldwide in terms of cybercrime.⁴ Nonetheless, cybercrime domination in Nigeria has been growing at an

¹ Proshare, Cybercrime in Nigeria: Cause and Effects, <https://proshare.co/articles/cybercrime-in-nigeria-causes-and-effects>.

² Augustine C. Onuora, The Challenges of Cybercrime in Nigeria An Overview, https://www.academia.edu/41472768/The_Challenges_of_Cybercrime_in_Nigeria_An_Overview.

³ *Id.* at 5-6.

⁴ Pelumi O. Apantaku, Cybercrime- Motivations, Modes, and Emerging Trends with Nigeria as a Case Study, https://pure.port.ac.uk/ws/portalfiles/portal/43107560/Final_Thesis.pdf.

unprecedented rate for years, to the point that it may erode the power of wealthy countries such as the United States and the United Kingdom.⁵

The Nigerian “national” administration has failed to appropriately respond to cybercrime, which is reinforced by bureaucracy, a lack of control power, and inexperienced law enforcement. Furthermore, the government has not devoted time, money, or study to the subject, whereas other nations have worked to expand intervention or transform the cybercrime community into cybersecurity communities, as well as develop legal initiatives for cybercriminals.⁶ However, the Nigerian government faces other challenges, such as organized crime and terrorism, that constrains the government’s ability to commit fully in resolving this issue.

Despite these difficult trends in Nigeria, the most recent presidential election demonstrated the Nigerians' willingness to use democratic means to express their desire to improve the country, such as economic and workforce development.⁷ Many have expressed their energetic voices to speak out and protest the current economic condition as well as other social issues. Youths have expressed the need for assistance with a developed pathway from school to post-graduate employment. People have fought back when dealing with corruption in law enforcement and certain controversial government policies. One notable character trait of Nigerians is their resilience to life. No matter the circumstances, they will be resilient and find a way. Jane Abieyuwa Igharo, a Nigerian Canadian fiction writer, said, “*To Nigerians*

⁵ *Id.*

⁶ *Id.*

⁷ Nimi Princewill, Stephanie Busari, Nigeria is about to hold Africa's largest democratic exercise. Here's what to know about its presidential election, <https://www.cnn.com/2023/02/21/africa/nigeria-presidential-poll-2023-intl-cmd/index.html>.

everywhere—at home and in the diaspora. I am in awe of your talent, resilience, and innovation. I dey hail una.”⁸

My paper will address the issue of cybercrime in Nigeria and the possibility of creating a cybersecurity initiative program for cybercriminals to use their skills for good practice for themselves and the country as well.

II. Background Information

Nigeria has produced the most talented people molded by their work ethic and grit.⁹ However, due to the nonchalance of the government, most of them must figure it out on their own with the resources around them. Many underappreciated bright Nigerians have maneuvered their way into bad behaviors such as gambling, drug selling, and cybercrime because of undeserved efforts.¹⁰ This has caused them to dim their passions and channel their frustrations into illegal activities. This section will discuss the situation of cybercrime in Nigeria and how it has infiltrated Nigerians and serves as a means for them due to the government's lack of assistance.

a. The State of Cybercrime in Nigeria

Cybercrime is referred to as a criminal activity involving the use of a computer, network, or networked device. Cybercrime is committed generally by hackers looking to make a financial gain. With the world becoming a global village and the advancement of the Internet and Communications Technologies, cybercrime is increasingly being used for nefarious purposes as

⁸ Goodreads, Jane Igharo-Quotes, https://www.goodreads.com/author/quotes/19841781.Jane_Igharo.

⁹ Hashim Yussuf Amao, Nigeria: A Realm of Uncelebrated Talents, <https://www.thenews-chronicle.com/nigeria-a-realm-of-uncelebrated-talents/>.

¹⁰ *Id.*

the Internet becomes increasingly reliant as a critical infrastructure.¹¹ Specifically, cybercrime in Nigeria has produced a breeding ground for a variety of malicious practices. In recent years, many criminal elements in this country have used modern network infrastructure, such as the Internet and mobile phones, to commit a variety of international fraudulent crimes (e.g., vishing, phishing, ransomware, software piracy, etc.) that ultimately hurt Nigeria's global reputation. Such crimes also jeopardize the country's safety and economic well-being.¹²

Throughout Nigeria's modern history, cybercrime had an evolving role that provided different opportunities for threat actors. Initially, cybercrime involved the use of information that provided financial support to facilitate traditional crimes. It took advantage of accessing vast cyber networks to further the extent of criminal enterprises that lead to the kidnapping or auctioning of illegal items.¹³ Presently, many criminal activities are based solely on the Internet, which sometimes makes it difficult for law enforcement to detect and prosecute such unlawful operations. Furthermore, cybercrime has been linked to high unemployment rates, solidifying the old proverb popular in Nigeria that "an idle mind is the devil's workshop," as millions of unemployed people have turned to cybercrime in hopes of enhancing their livelihood and staying afloat.¹⁴ The prevalence and success of various cybercrime operations will encourage the

¹¹ Temitayo Bello, Anatomy of Cybercrime in Nigeria: The Legal Chronicle, <https://deliverypdf.ssrn.com/delivery.php?ID=785068073073026082117012105074100007098032068060033065078103094014098126031104090031057121038126047045032096112100019081090000031033007080032015003006028117109004099000006020124070113091104084105121100101005100094075100119066089090122064106106072112021&EXT=pdf&INDEX=TRUE>.

¹²Augustine C. Onuora, The Challenges of Cybercrime in Nigeria An Overview, https://www.academia.edu/41472768/The_Challenges_of_Cybercrime_in_Nigeria_An_Overview.

¹³ Catherine Nicholls, Nigerian senator guilty of organ harvesting plot, UK court rules, <https://www.cnn.com/2023/03/23/uk/nigerian-senator-organ-harvesting-intl-gbr/index.html>.

¹⁴Augustine C. Onuora, The Challenges of Cybercrime in Nigeria An Overview, https://www.academia.edu/41472768/The_Challenges_of_Cybercrime_in_Nigeria_An_Overview.

younger generation to participate in cybercrime activities. This problem is compounded by multiple Nigerian entertainment and social influences constantly providing news on displaying “yahoo” (scam artists who participate in fraudulent activities) activity in a positive light.

b. The Current Nigerian Cybercrime Trends

There are various ways in which cybercrime is manifested in Nigerian culture. The well-known colloquial term "419" or "Yahoo Yahoo" refers to cyber miscreants who specialize in various internet crimes. It began with individuals defrauding people via physical authentic-looking mail to modern email and other social media networks. Some successful 419s used their highly technical skills for criminal purposes, which led to luxurious lifestyles funded by crime. A "Yahoo boy" can be identified quickly by his distinctive style of clothing and excessive spending on materialistic things.¹⁵

Phishing is another commonly used cybercrime technique that is especially popular in Nigeria.¹⁶ Typically, attackers would clone e-commerce sites or products to deceive unsuspecting users. This technique frequently uses random emails to trick people into disclosing financial and/or personally identifiable information.¹⁷ In addition, cybercrime on different levels has affected multiple industries. For example, the telecommunications sector has been a victim of individuals using “cheat codes” to access illegally unlimited mobile telephone airtime. In another example, the entertainment industry is threatened by digital piracy, which hurts the

¹⁵ Pelumi O. Apantaku, Cybercrime- Motivations, Modes, and Emerging Trends with Nigeria as a Case Study, https://pure.port.ac.uk/ws/portalfiles/portal/43107560/Final_Thesis.pdf.

¹⁶ Augustine C. Onuora, The Challenges of Cybercrime in Nigeria An Overview, https://www.academia.edu/41472768/The_Challenges_of_Cybercrime_in_Nigeria_An_Overview.

¹⁷ *Id.*

growth of the Nigerian music industry and intellectual property on domestic and foreign works of art.¹⁸

Cybercrime also affected the Nigerian government. In 2015, the Nigerian Electoral College website and other government websites were defaced, affecting the government's ability to provide services across Nigeria. Much of the country's cybercrime is supported by a complex and sophisticated skill-based workforce, many of whom are Black-Hat Hackers (who are hackers that maliciously breach into computer networks).

The significant feature Nigeria's widespread cybercrime activities can be rooted to the lack of opportunities for entering the cybersecurity workforce. Nigeria is a breeding ground for untapped and brilliant talent, especially in the technical field. However, the country lacks robust cybersecurity and other technical workforce pipelines, which limits *legitimate* economic opportunities for technically skilled Nigerians. As such, one cannot easily blame cybercriminals for engaging in these unlawful activities due to the economic circumstances created by the government. But if individuals were given the opportunity to produce excellent performance from their high technical skills, they may repurpose their talents for legitimate purposes and improve the country's socioeconomic state.

III. Transition From Cybercrime to Cybersecurity Workforce

The world is entering a new era of emerging internet dependence. Major changes in the coming years will unlock new opportunities for human well-being and affluence. For example, internet-of-things devices have extended functionality of everyday appliances, giving time-saving features to enhance day-to-day lives. However, those changes also introduce new or

¹⁸ Pelumi O. Apantaku, Cybercrime- Motivations, Modes, and Emerging Trends with Nigeria as a Case Study, https://pure.port.ac.uk/ws/portalfiles/portal/43107560/Final_Thesis.pdf.

enhance existing systemic risks posed by poor security frameworks. Focusing on internet-of-things devices, poor cybersecurity practices may allow threat actors to use internet-of-things devices as entry points to access protected networks.

Technology was initially created to facilitate digital growth, promote free speech, and provide a space to foster innovation. Unfortunately, technology has also been used for malicious activities, especially criminal cyber activities that have been enabled by societal and economic effects. Technology and human beings are becoming interconnected, introducing both the benefits and problems arising out of the digital ecosystem.¹⁹ This can be applicable to the Nigerian infrastructure and economic situation. For example, a lot of Nigerians have independently created a sustainable lifestyle for themselves because the government and its policies failed to provide adequate resources to the nation at large. However, there is an opportunity for technically-minded Nigerians—many of whom have placed their motivation in the wrong mindset (i.e., many technically savvy Nigerians participating in cyber gangs)—to repurpose their valued cyber skills in legitimate industries. This workforce transformation can lead to the uplifting of the nation’s security, economic and global status.

a. Government Engagement and Funded Cybersecurity Programs

For a nationwide cyber workforce transformation to happen, a strategy focusing on turning cybercriminals skills into a profitable profession must be developed. The main goal of this strategy should be creating programs and providing economic initiatives to facilitate the transformation process. One of the aims should focus on providing deep collaboration among the

¹⁹ The White House, FACT SHEET: Biden Harrison Administration Announces National Cybersecurity Strategy, <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/>.

people, the government, and the public/private sectors. Investing in the lives of talented cyber-skilled individuals will prepare Nigeria as the next-generation leader in technology.

This workforce development approach has been used in other countries, including the U.S. in its *2023 U.S. National Cybersecurity Strategy*. According to the U.S. National Cybersecurity Strategy's fourth pillar, the U.S. government leverages investments in programs and *nationally funded* initiatives to produce outcomes that are both financially sustainable and beneficial to the country's interest.²⁰ Following U.S.'s approach, the Nigerian national government must utilize equitable public investments to establish new grant programs available to all thirty-six Nigerian states.

Creating a research program community that prioritizes proactively preventing and mitigating cybersecurity risks in current and next-generation technologies²¹ will improve Nigeria's national security infrastructure and make it possible for students and graduates to start obtaining employment experiences that should align with their desired technological area. Furthermore, the Nigerian government partnering with public and private entities, can develop programs to create a full-time cybersecurity employment pipeline to foster a professional relationship and commitment among potential employees and employers.

b. Government Diversity Recruitment Efforts

Another reason for investing in a cybersecurity community is to protect the public cyber infrastructure both within the country and globally. The Internet is a vulnerable place, and the risk of exposure grows by the day.²² With new vulnerability exposure, steps must be taken to mitigate the pervasive concerns (e.g., bank fraud, network intrusions, and link dupes). Who

²⁰ *Id.*

²¹ *Id.*

²² *Id.*

better hire people who have the expertise and can put their skills to good use? Perhaps, Nigerians themselves.

Taking similar workforce development approaches of the U.S., the Nigerian federal government can take the lead by utilizing a vibrant Nigerian cyber workforce to ensure the networks are secure while also collaborating with other entities and organizations to develop and implement measures to improve the nation's digital infrastructure.²³ In addition, having the cyber workforce inclusive—regardless of tribal affiliation or prior acts of nepotism—is needful to combat the additional barriers to the unemployment issue in the country. This way, the national government is uniting technical talent from all parts of Nigeria to combat the nation's cybersecurity issue. In addition, it produces a new economic flow to the country and builds stronger relationships with the neighboring African countries by providing potential cyber techniques and solutions, which may mitigate dependency on foreign, non-African contractors, usually from the Western and Asian regions. In the long term, this will set up Nigeria to be ready for an upgraded digital infrastructure and a vibrant cybersecurity services industry that the country can provide services throughout the African continent.

IV. Conclusion

Nigeria has a large pool of untapped talent that goes unused, and the government's lack of focused assistance magnifies this effect. The government has the opportunity to identify the problem, devise a solution, and even discuss policy implementation. Yet none of this effort will matter unless a proactive effort is made to boost the nation's in-house cybersecurity capabilities by investing in its people.

²³ *Id.*

Previous efforts have developed plans to combat cybercrime by bringing in new technological solutions but failing to implement fully the proposed plan.²⁴ This paper's solution is to create an environment in which underdeveloped talent may thrive and put their incredible skills to good use. As a Nigerian American immigrant who has witnessed precisely what the government has done to its communities, I am appalled by the imbalance and scarcity of resources that many people lack. Yet, it is up to Nigerians, including those in government and those exerting great influence, to do what is right and serve the country.

²⁴ Uche Igwe, Nigeria's growing cybercrime threat needs urgent government action, <https://blogs.lse.ac.uk/africaatlse/2021/06/09/nigerias-growing-cybercrime-phishing-threat-needs-urgent-government-action-economy/>.

WORK CITED

1. Proshare, Cybercrime in Nigeria: Cause and Effects, <https://proshare.co/articles/cybercrime-in-nigeria-causes-and-effects>.
2. Augustine C. Onuora, The Challenges of Cybercrime in Nigeria An Overview, https://www.academia.edu/41472768/The_Challenges_of_Cybercrime_in_Nigeria_An_Overview.
3. Pelumi O. Apantaku, Cybercrime- Motivations, Modes, and Emerging Trends with Nigeria as a Case Study, https://pure.port.ac.uk/ws/portalfiles/portal/43107560/Final_Thesis.pdf.
4. Nimi Princewill, Stephanie Busari, Nigeria is about to hold Africa's largest democratic exercise. Here's what to know about its presidential election, <https://www.cnn.com/2023/02/21/africa/nigeria-presidential-poll-2023-intl-cmd/index.html>.
5. Goodreads, Jane Igharo-Quotes, https://www.goodreads.com/author/quotes/19841781.Jane_Igharo
6. Hashim Yussuf Amao, Nigeria: A Realm of Uncelebrated Talents, <https://www.thenews-chronicle.com/nigeria-a-realm-of-uncelebrated-talents/>.
7. Temitayo Bello, Anatomy of Cybercrime in Nigeria: The Legal Chronicle, <https://deliverypdf.ssrn.com/delivery.php?ID=785068073073026082117012105074100007098032068060033065078103094014098126031104090031057121038126047045032096112100019081090000031033007080032015003006028117109004099000006020124070113091104084105121100101005100094075100119066089090122064106106072112021&EXT=pdf&INDEX=TRUE>.
8. Catherine Nicholls, Nigerian senator guilty of organ harvesting plot, UK court rules, <https://www.cnn.com/2023/03/23/uk/nigerian-senator-organ-harvesting-intl-gbr/index.html>.
9. The White House, FACT SHEET: Biden Harrison Administration Announces National Cybersecurity Strategy, <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/>.

10. Uche Igwe, Nigeria's growing cybercrime threat needs urgent government action, <https://blogs.lse.ac.uk/africaatlse/2021/06/09/nigerias-growing-cybercrime-phishing-threat-needs-urgent-government-action-economy/>.