

Tackling Cybercrimes in the 5G Era: An Examination of the Readiness and Digital Skills of the Nigerian Police

Christopher Nkiko, Elizade University, Ilara-Mokin, Nigeria

Edwin Iroeroavwo Achugbue, Delta State University, Abraka, Nigeria

Omorodion Okuonghae, Samuel Adegboyega University, Ogwa, Nigeria

ABSTRACT

The study examined the readiness and digital skills of the Nigerian Police in tackling cybercrimes in the 5G era. Consequently, four specific research objectives were identified, and three hypotheses were tested in the study. The descriptive correlational research design was adopted for the study and the population comprised all police officers from the rank of Assistant Superintendent of Police (ASP) and above in the Criminal Investigation Department in Edo State (including the Anti-Fraud Unit). The sample for the study was 35 police officers in the state. The instruments for data gathering was self-designed questionnaire, and the data collected were analyzed using both descriptive and inferential statistics. From the data analyzed, it was gathered that significant relationship existed among the readiness, digital skills of the Nigerian Police, and the tackling of cybercrimes in 5G era. The study concluded that the deployment of 5G technology will bring with it a new level of cyber threat, which will truly test the resolve of cyber security in and outside the country.

KEYWORDS

5G, 5G Era, Cybercrime, Digital Skills, Internet Fraud, Nigerian Police, Readiness, Telecommunication

INTRODUCTION

The 21st century has witnessed the widespread adoption of internet and other information technologies in different sectors in Nigeria. This widespread adoption led to the rise of diverse cybercrimes in and outside Nigeria. Cybercrimes simply refers to criminal activities such as fraud, theft, forgery, blackmail and malicious codes carried out using information technology or the Internet network (Omodunbi, Odiase, Olaniyan, & Esan, 2016). Cybercrimes evolve from the abuse or wrong application of computer systems and network. These abuses usually pose great danger to the person, groups or organizations against whom the crime is committed.

In Nigeria, cybercrimes are committed in different sectors of the economy such as in banking (with crimes such as BVN scams, phishing, Credit Pin/card theft, and banking fraud), E-commerce (software piracy- intellectual property theft, sales fraud and forgery, data and airtime theft from service providers), Education (cyber plagiarism and cyber pornography), and social media sector (cyber stalking, harassment and blackmailing scam, social hijacking, identity theft and cyber bullying).

DOI: 10.4018/IJICTRAME.2020070105

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

These criminal activities have increased exponentially in Nigeria, especially within the last decade. In a 2016 ranking of countries with the highest cyber-attacks vulnerabilities by CheckPoint, a global network cyber security vendor, Nigerian was ranked 16th highest. This implies that Nigeria is highly susceptible to cyber-attacks in different sectors. This is evident in the high number of reported cases of cybercrimes in Nigeria as well as cybercrimes committed by Nigerians outside Nigeria (Olayemi, 2014). However, cyber security expert, Bayern (2018), expressed fear that cybercrimes may increase with the deployment of 5G technologies.

5G technology is a fifth generation wireless network architecture which is built to enable superior data communication rate between wireless area networks (Technopedia, 2019). The technology is designed to greatly increase speed and responsiveness of wireless networks in addition to providing network management features. Loughran (2019) noted that 5G technology will promote the widespread implementation of Internet of Things (IoT) technology and other next generation network. Using the 5G technology, network operators can deliver 5G fixed wireless broadband services and 5G cellular services. However, despite the numerous advantages that accompany the deployment of 5G technologies, there are widespread concerns that cybercrimes will be exacerbated by 5G. Cyber security experts such as Loughran (2019) and Samani (2019) have expressed deep concern that the introduction of 5G technologies could increase the amount of data, criminals could steal from consumers and businesses. It is anticipated that the existing cyber security will be greatly threatened in a 5G-connected world. As Willet (2019) put it:

5G technology can also enable the weaponisation of Internet of Things (IoT) devices in botnet attacks. By allowing more devices to connect, 5G can potentially enable them to become part of a malicious botnet, through which hackers can launch powerful Distributed Denial of Service (DDoS) attacks (p.1).

Furthermore, Bayern (2018) asserted that, with the speed and connectivity of 5G, poor hygiene users of internet will most likely have several security issues to deal with, thus, translating to wide spread of cybercrimes since the average internet users are still making basic security errors such as using same password in multiple places and clicking fraudulent links. In addition, the deployment of 5G network will lead to storing large amount of data in the cloud rather than on a more secure local server, thus, giving room for vastly expanded attack surface.

In order to tackle the cybercrimes that would arise with the deployment 5G in Nigeria, the Nigerian Police, being a law enforcement agency, must work closely with cyber security agency and other agencies such as the National Information Technology Development Agency (NITDA) and the Nigerian Communications Commission (NCC) if they are to effectively tackle cybercrimes in Nigeria. Also the Nigerian Police must demonstrate complete readiness in tackling cybercrimes in 5G era. They must have a good understanding of how the technology works in 5G era while also having the necessary digital skills to combat the crimes. It is on this note that this study examined the readiness and digital skills of the Nigerian Police in tackling cybercrimes in 5G era.

Problem Statement

The widespread development and deployment of technologies in different sectors in recent times has led to the consistent growth of cybercrimes in Nigeria and the world at large. In Nigeria for instance, there has been consistent reported cases of data theft, E-mail spoofing, cyber defamation, website cloning, malicious computer codes, web jacking, Phishing, identity theft, cyber trespass and cyber fraud. More recently, there were reported cases of FBI nabbing high profile Nigerians for fraudulent activities within the cyberspace. These criminal activities have continued to dent the image of Nigeria in the international scene.

Sadly, there have been speculations that cybercrimes will increase exponentially with the launching of 5G network in Nigeria. To address this issue in Nigeria, the Nigerian Police, being a law enforcement agency, must demonstrate that they are ready (physically and mentally) as well as

11 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:

www.igi-global.com/article/tackling-cybercrimes-in-the-5g-era/259889?camid=4v1

This title is available in InfoSci-Journals, InfoSci-Journal Disciplines Business, Administration, and Management, InfoSci-Journal Disciplines Computer Science, Security, and Information Technology, InfoSci-Computer Science and IT Knowledge Solutions – Journals, InfoSci-Business Knowledge Solutions – Journals. Recommend this product to your librarian:

www.igi-global.com/e-resources/library-recommendation/?id=2

Related Content

The Use of Information and Communication Technology for the Preservation of Aboriginal Culture: The Badimaya People of Western Australia

Katina Michael and Leone Dunn (2007). *Information Technology and Indigenous People* (pp. 170-174).

www.igi-global.com/chapter/use-information-communication-technology-preservation/23550?camid=4v1a

Management Game: Gamifying Leadership Learning

Marko Kesti, Aino-Inkeri Ylitalo and Hanna Vakkala (2019). *International Journal of Innovation in the Digital Economy* (pp. 37-52).

www.igi-global.com/article/management-game/227368?camid=4v1a

Are We There Yet?: An Exploratory Predictive Study of Instructor Acceptance of an Educational Tablet Computer

Stephen Asunka (2016). *International Journal of E-Adoption* (pp. 35-49).

www.igi-global.com/article/are-we-there-yet/160140?camid=4v1a

Sharing and Avatar-Based Innovation Tools on Digital Economy Perspectives Using Levy Processes Simulation: Modelling in the Globalization Era

Vardan Mkrttchian and Yulia Vertakova (2020). *International Journal of Innovation in the Digital Economy* (pp. 52-63).

www.igi-global.com/article/sharing-and-avatar-based-innovation-tools-on-digital-economy-perspectives-using-levy-processes-simulation/256153?camid=4v1a