Journal of Applied Sciences, Information, and Computing
Vol. 3, No. 1 (June, 2022)

ISSN: 1813-3509 **https://jasic.kiu.ac.ug**

Understanding the Challenges of Tackling Cybercrime Activities in the Era of 5G Technology

Dr. Musa Ahmed Zayyad[1], Amina Lawal[2]
[1]Department of Information Technology, School of Mathematics & Computing, Kampala International University Uganda. zayyad.musa@kiu.ac.ug
[2]Department of Computer Science, School of Sciences, Federal College of Education Katsina State – Nigeria. meenalawal@yahoo.com

Abstract
Context: Deployment of 5G wireless technology has taken place in some developed and developing countries. The technology is expected to provide faster speed, greater reliability, low latency, in addition to opening up a new sphere of possibilities such as connected vehicles and devices. However, despite the expectation of improvements promised in the 5G era when compared to previous mobile wireless technologies such as 4G and 3G, there is a growing concern within the ICT industry that there are a number of security issues, particularly cybercrime attacks that may likely become rampant due to the power of the 5G technology. ICT experts agrees that 5G technology will result in massive data transactions due to the ultra-high speed, low latency and extra capacity provided by these networks. Therefore, there is the need to ensure that data and transactions are secured in such a way that personal information is not hacked, data privacy is preserved, and systems do not crash.
Objective: The objective of this study is to analyze the critical challenges in combating cybercrime activities in the era of 5G technology. The paper will look at the security issues in the 4G networks and then compare it with the upcoming technologies expected in the 5G era.
Method: The paper uses secondary data that was obtained by reviewing relevant articles written by various scholars on the topics of 5G technology, 4G technology, cybercrime activities in the era of 4G, how cybercrime will be tackled in the era of 5G technology, as well as evolution of mobile generation technologies from 1G to 5G.
Results: The study highlighted a better understanding of cyber security threats, attacks, vulnerability in the 4G technology era and suggested a number of ways to deal with them and help to implement a secure information platform in the era of the technology.

Keywords: 4G, 5G, Cybercrime, Security, Technology, Wireless.

1. Introduction

The 5G technology is a generation that is currently under development, which is designed to improve on 4G. The 5G technology promises significantly faster data rates, higher connection density, much lower latency, among other improvements. Some of the plans for 5G include device-to-device communication, better battery consumption, and improved overall wireless coverage. There has been a vast advancement in mobile wireless communication since the last few decades. This innovation consists of a number of generations and is still going on. The journey of mobile wireless communication began with 1G followed by 2G, 3G, 4G, and under research upcoming generations 5G. In the last few decades, Mobile Wireless Communication networks have experienced a remarkable change (Mitra & Agrawal, 2015).

The mobile wireless Generation (G) generally refers to a change in the nature of the system, speed, technology, frequency, data capacity, latency etc. Each generation have some standards, different capacities, new techniques and new features which differentiate it from the previous one. The first generation (1G) mobile wireless communication network was analog used for voice calls only. The second generation (2G) is a digital technology and supports text messaging. The third generation (3G) mobile technology provided higher data transmission rate, increased capacity and provide multimedia support. The fourth generation (4G) integrates 3G with fixed internet to support wireless mobile internet, which is an evolution to mobile technology and it overcome the limitations of 3G. It also increases the bandwidth and reduces the cost of resources (Reddy, Jaswanth & Pramod, 2016).

5G stands for 5th Generation Mobile technology and is going to be a new revolution in mobile market which has changed the means to use cell phones within very high bandwidth. User never experienced ever before such high value technology which includes all type of advance features and 5G technology will be most powerful and in huge demand in near future. Mobile communication has become more popular in last few years due to fast reform from 1G to 5G in mobile technology. This reform is due to requirement of service compatible transmission technology and very high increase in telecoms customers. Generation refers to change in nature of service compatible transmission technology and new frequency bands. In 1980 the mobile cellular era had started, and since then mobile communications have undergone considerable changes and experienced massive growth (Le et al., 2015).

Simply, the "G" stands for "GENERATION". While you connected to internet, the speed of your internet is depends upon the signal strength that has been shown in alphabets like 2G, 3G, 4G, etc. right next to the signal bar on your home screen. Each Generation is defined as a set of telephone network standards, which detail the technological implementation of a particular mobile phone system. The speed increases and the technology used to achieve that speed also changes. For e.g., 1G offers 2.4 kbps, 2G offers 64 Kbps and is based on GSM, 3G offers 144 kbps-2 mbps whereas 4G offers 100 Mbps - 1 Gbps and is based on LTE technology .

The aim of wireless communication is to provide high quality, reliable communication just like wired communication (optical fibre) and each new generation of services represents a big step(a leap rather) in that direction. This evolution journey was started in 1979 from 1G and it is still continuing to 5G. Each of the Generations has standards that must be met to officially use the G terminology. There are institutions in charge of standardizing each generation of mobile technology. Each generation has requirements that specify things like throughput, delay, etc. that need to be met to be considered part of that generation. Each generation built upon the research and development which happened since the last generation. 1G was not used to identify wireless technology until 2G, or the second generation, was released. That was a major jump in the technology when the wireless networks went from analog to digital. Table 1 shows a comparison of all the mobile generation technologies from first generation to the fifth.

Table 1: Comparison of all mobile generation technologies 1G – 5G

Technology ⟹ Feature ⇩	1G	2G	3G	4G	5G
Start/ Deployment	1970 – 1980	1990 – 2004	2004-2010	Now	Soon (probably 2020)
Data Bandwidth	2kbps	64kbps	2Mbps	1 Gbps	Higher than 1Gbps
Technology	Analog Cellular Technology	Digital Cellular Technology	CDMA 2000 (1xRTT, EVDO) UMTS, EDGE	Wi-Max LTE Wi-Fi	WWWW(coming soon)
Service	Mobile Telephony (Voice)	Digital voice, SMS, Higher capacity packetized data	Integrated high quality audio, video and data	Dynamic Information access, Wearable devices	Dynamic Information access, Wearable devices with AI Capabilities
Multiplexing	FDMA	TDMA, CDMA	CDMA	CDMA	CDMA
Switching	Circuit	Circuit, Packet	Packet	All Packet	All Packet
Core Network	PSTN	PSTN	Packet N/W	Internet	Internet

[**Source:** Sharma (2013) – Date accessed 11th February, 2022]

1.1. Aims and Objectives

The aim of this paper is to highlight and discuss the concept of cybercrime and its effects on individuals, organizations, the society, and countries at large. The paper also highlights the types of cybercrime, classification of cybercrime victims and attackers, reasons for engaging in cybercrime activities, and preventive measures that needs to be put in place by cybercrime victims to avoid cybercrime attack.

1.2. Research Questions

Based on the effect of cybercrime committed by cyber criminals and the victims involved in the cyber-attack, this paper has put forth the following strategic research questions, which include:

a) What are the ways in which cybercrimes are committed?
b) Who are the cyber criminals and the cybercrime attack victims?
c) How can the cybercrime be reduced or prevented?
d) What is the level of cybercrime awareness by internet users?

However, the need to be careful and vigilant is paramount in the present circumstances. It is possible to safely use the internet by taking some simple measures to mitigate the risks of the cybercrime.

2. Methodology

In the course of this study, the data for this paper was obtained from secondary sources that include excerpts from books, reports, and literatures from scientific databases such as Science Direct, IEEE, and Google Scholar. Reports from news media and news portal were also considered. The paper reviewed relevant articles written by various scholars on the topics of 5G technology, 4G technology, and cybercrime activities in the era of 4G, how cybercrime will be tackled in the era of 5G technology, as well as evolution of mobile generation technologies from 1G to 5G. The paper considered only those articles that were published recently and by reputable journal publishers. Also, information was obtained from consultations with internet users and information technology (IT) experts about their knowledge and experiences of cybercrime activities.

3. Related Literature Review

Most cybercrimes cannot be placed into a single crime category, which makes statistical recording of this activity limited at best. The Internet Crime Complaint Center (IC3) compiles and releases annual reports on the statistics and cybercrime facts. Using statistics and facts, analysts prepare reports on cybercrime trends and growth (Internet Crime Report, 2011).

Knowing the facts, trends, and growth is critical to crime prevention efforts on protecting personal data in public and private sectors. This also helps in the creation of tools and strategies to combat cyber criminals. Internet connected activities are as vulnerable to crime and can lead to victimization as effectively as common physical crimes. The types of crimes that are currently occurring have existed long before the Internet was around. By virtue of the tools being used today to commit cybercrimes, criminals are now more anonymous and provided with a virtual market of available victims. The responsibility falls on individuals to protect themselves and their families through safe online practices.

The internet proliferation in Nigeria brought about many developmental changes in the field of ICT. Various technology activities that were unknown before have become very popular nowadays, such as e-banking, e-commerce, e-health, cloud computing to mention but a few. However, this ICT development brought about an exceptional outbreak of cybercrime, which has negative impact on the socio-economy of the country, and also affects its image in the international community (Olusola et al., 2013).

Over the past few years, Nigeria has acquired a global notoriety in cybercrime activities, ranging from financial scams, ATM frauds, phishing, identity theft, which is all facilitated through the use of internet (Moses-Òkè, 2012). Nigeria's economic vitality and national security depend on a vast array of interdependent and critical networks, systems, services, and resources known as cyberspace. Cyberspace has transformed the ways we communicate, travel, run our economy, and obtains government services. Nigerian cyber criminals are daily devising new ways of perpetrating this form of crime and the existing methods of tracking these criminals are no longer suitable for to deal with their new tricks. The victims as well show increasing naivety and gullibility at the prospects incited by these fraudsters (Hassan et al., 2012).

According to statistics, Nigeria is ranked 3rd among 10 nations with the worst record of cyber-crime activities in the world. Various measures were put in place to contain the acts, such as the setting up of National Cyber security initiative in 2003. This agency was

mandated to collaborate with the Nigerian Cybercrime Working Group to realize its objectives of reducing or eliminating the cybercrime (Olayemi, 2014). However, not much success has been achieved, because the rate of growth of the cybercrime continued to rise, with new methods and tricks being devised by the cyber criminals. Cybercrime is very complex to deal with, because it is mostly committed from remote locations that are very difficult to monitor, and the absence of relevant laws and liabilities makes it the more difficult to monitor.

3.1. What is Cybercrime?

Human being has been associated with crime and criminality since the Stone Age. Different kinds of criminal activities are being committed by individuals, group of people, organizations, companies, and countries in one way or the other. Various kinds of strategies are being put in place to contend with crime according to their nature and extent. According to (Dashora, 2011), high rate of crime can hamper the development efforts of organizations and countries, because crime is considered as the direct opposite of nation building. It has negative social and economic consequences. As information and communication technologies (ICT) becomes ubiquitous through the use of internet, electronic crime known as cybercrime becomes rampant, where people and organizations were attacked, countries are engaged in cyber war, sensitive information being stolen or tempered with, individuals' privacy being invaded, and numerous other security threats happening daily.

Cybercrime is defined as crimes taking place through the internet using computers, Smartphones, and other communication technologies (Balogun & Obe, 2010). Cybercrime can be as high as stealing huge sums of money or sensitive records to as low as sending unsolicited spam email messages in form of advertisement and the victims of the attack usually involved individuals, organizations, or countries. In most cases, the victims of cybercrimes do not report the incidences as a result of stereotype, and those who engaged in cybercrime often pride themselves of having skilled internet knowledge with the believe that they are not criminals (Okeshola & Adeta, 2013).

According to Ehimen and Bola (2010), cybercrime is any crime committed or facilitated via the Internet, which involves using human beings, computers, and networks as tools or victims of an attack. Cybercrime activities incorporates anything from stealing millions of dollars from online bank accounts, distant theft of government or corporate secrets, criminal trespass into remote systems around the globe, to non-money offenses such as creating viruses on other computers, downloading illegal music files, posting confidential business information on the Internet, or sending unsolicited emails (spam) as advertisement.

Governments have long engaged in criminal activity directly, or have sought the assistance of cyber criminals to do their "dirty work" for them. Studies have shown that various governments (or their proxies) are using Internet technologies to commit crime (Broadhurst et al., 2014). The United States of America and Russia has often accused each other of committing cybercrime attack. The Chinese intelligence services were alleged to be involved in widespread economic and industrial espionage for their selfish advantage. Based on the revelation made by Edward Snowden, the United States Government has engaged in massive programs of cyber-surveillance that were targeted at powerful individuals, companies, and countries in general. One might also note the offensive cyber operations against Iranian nuclear enrichment facilities (Terrill, 2013). Such activities may not be defined as criminal under the laws of the state that undertakes them, but are usually regarded as crimes by the state that is on the receiving end, and the activities in question are nothing, if not organized.

3.2. Cybercrime in the Era of 4G

Although cybercrime is regarded as a global phenomenon, there are however some cybercrime activities that occurs more frequently in Nigeria. The following are some of the cybercrimes committed in Nigeria (Adeniran, 2008):

a) **Beneficiary of a Will Scam**: The criminal sends e-mail to claim that the victim is the named beneficiary in the will of an estranged relative and stands to inherit an estate worth millions.

b) **Online Charity**: Another aspect of e-crime common in Nigeria is where fraudulent people host websites of charity organizations soliciting monetary donations and materials to these organizations that do not exist. Unfortunately, many unsuspecting people have been exploited through this means.

c) **Next of Kin Scam**: Collection of money from various bank and transfer fees by tempting the victim to claim an inheritance of millions of dollars in a Nigerian bank belonging to a lost relative.

d) The "Winning Ticket in Lottery you Never Entered" Scam: These scams lately include the State Department's green card lottery.

e) Bogus Cashier's Check: The victim advertises an item for sale on the Internet, and is contacted.

f) Computer/Internet Service Time Theft: Whiz kids in Nigeria have developed means of connecting Cyber Cafes to Network of some ISPs in a way that will not be detected by the ISPs and thereby allow the Cafes to operate at no cost.

g) Lottery scam: Allowing users believe they are beneficiaries of an online lottery that is in fact a scam.

3.3. Cybercrime Protective Measures

Cyber criminals are no different than traditional criminals in that they want to make their money as quickly and easily as possible. Cybercrime prevention can be achieved fairly quickly and in a cost-effective manner. When armed with a little technical advice and common sense, many cybercrime attacks can be avoided. Cyber security is the measure put in place to protect the cyberspace. If a cyber-criminal finds it very difficult to attack a particular target due to strong preventive measures, he/she then moves along and find an easier target.

The following are some of the security measures that can be put in place to prevent an attack from cyber-criminal (Ayofe & Oluwaseyifunmitan, 2009):

a) **Keep the computer system up to date:** Cybercriminals will use software flaws to attack computer systems frequently and anonymously. Most Windows-based systems can be configured to download software patches and updates automatically. By doing this, cyber-criminals who exploit flaws in software packages may be thwarted. This will also deter a number of automated and simple attacks criminals use to break into your system.

b) **Protect your personal information:** Using many of the online services today involves sharing basic personal information to include name, home address, phone number, and email address. Using common sense is the best way to protect against and prevent cybercrime. Before you disclose your personal information on any website, check the security features of the website to ensure that it is secure. Any financial transaction website should have an "s" after the letters "http" (e.g., https://www.mystore.com not http://www.mystore.com). The "s" stands for secure and should appear when you are in an area requesting you to login or provide other sensitive data. Another sign that you have a secure connection is the small lock icon in the bottom of your web browser (usually the right-hand corner).

c) Read the fine print on website privacy policies: On many social networking and photo sharing sites, there is wording on the privacy policies that allow the website to keep information and photos posted to the site, sometimes indefinitely, even after the original has been deleted by the user. While this may not discourage one from posting images or messages, awareness that this can be later retrieved and disseminated may be a consideration as to what information or photos are posted. What today may seem to be a harmless prank can have a devastating effect on one's reputation several years later.

d) **Review financial statements regularly:** Reviewing credit card and bank statements regularly will often reduce the impact of identity theft and credit fraud by discovering the problem shortly after the data has been stolen or when the first use of the information is attempted. Credit card protection services can often alert a person when there is unusual activity occurring on his or her account, for example, purchases in a geographically distant location or a high volume of purchases. These alerts should not be taken lightly and could be the first indicator that a victim receives that something is wrong.

e) **If it seems too good to be true, it is:** No one is going to receive a large sum of money from a stranger, or win a huge lottery from being "randomly selected from a database of email addresses," or make big money from "passive residual income a few hours each day working out of your home." Many of these crimes go unreported because the victim is too embarrassed to admit to law enforcement that they were duped.

f) **Turn off your computer:** With the growth of high-speed Internet connections, many opt to leave their computers on and ready for action. The downside is that being "always on" renders computers more susceptible. Beyond firewall protection, which is designed to fend off unwanted attacks, turning the computer off effectively severs an attacker's connection, be it spyware or a botnet that employs your computer's resources to reach out to other unwitting users. The bottom line is for every preventative measure

that you take, you limit your chances for becoming a victim of cybercrime.

3.4. How Cybercrime will be tackled in the 5G Era

The fifth generation mobile technology is currently under development, and most mobile network operators are expected to begin offering the services in 2019 or 2020. However, it is generally believed that new technologies bring new challenges and 5G is not an exception. In fact, cyber security experts and analysts generally believed that the 5G technology could increase the amount of data criminals could steal from individuals and organizations. This could be made possible because the new 5G technology is expected to be 10 to 100 times faster than the 4G network technology, and will have much lower latency.

In addition to the speed, key technologies that are expected to be available in the era of 5G include but not limited to: Massive MIMO, millimeter wave, small cells, Li-Fi all the new technologies from the previous decade could be used to give 10Gb/s to a user, with an unseen low latency, and allow connections for at least 100 billion devices.

a) **Secure configuration of the system:** It is important that computers are configured to the security level that is appropriate and comfortable for the user. Too much security can have the adverse effect of frustrating the user and possibly preventing them from accessing certain web content. Using the *"help"* feature of the operating system can often address many of the questions in this area.

b) **Choose a strong password and protect it:** Usernames, passwords, and personal identification numbers (PIN) are used for almost every online transaction today. A strong password should be at least eight characters in length with a mixture of letters and numbers. Using the same password for various sites or systems increases the risk of discovery and possible exploitation. It is never a good practice to write a password down and leave it near the system it is intended to be used on. Changing a password every 90 days is a good practice to limit the amount of time it can be used to access sensitive information.

c) **Keep your firewall turned on:** A firewall helps to protect your computer from hackers who might try to gain access to crash it, delete information, or steal passwords and other sensitive information. Software firewalls are widely recommended for single computers. The software is pre-packaged on some operating systems or can be purchased for individual computers. For multiple networked computers, hardware routers typically provide firewall protection.

d) Install or update your antivirus software: Antivirus software is designed to prevent malicious software programs from embedding on your computer. If it detects malicious code, like a virus or a worm, it works to disarm or remove it. Viruses can infect computers without the users' knowledge. Most types of antivirus software can be set up to update automatically. Antivirus software is the next line of defence, monitoring all online activity with the intent to protect the system from viruses, and other malicious programs.

4. Conclusion

While 5G technology would be a revolution in the world of mobile wireless system and a step forward for users, it also came with risks. It is clear that growth in ICT has led to over reliance on technology to undertake basic as well as critical communication services amongst individuals, organizations and countries. It is not possible to eliminate cybercrime from the cyber space due to its nature. However, it is quite possible to check it and take precaution as highlighted by the paper. The fight against cybercrime and cyber security threats requires literacy of information technology as well as information technology intelligence by internet users'. The paper was able to highlight the concept of cybercrime, victims and attackers, and also recommends some strategic measures that need to be taken to reduce the effect of cybercrime.

5. Recommendations

a) Strong passwords: it is generally believed that using strong passwords on every account could reduce the menace of cybercrime.

b) Create massive awareness about the danger and risks of security and privacy that are integrated into every part of our daily activities.

c) Avoid disclosing any information pertaining to one self to avoid cyber-stalking. This is as good as disclosing your identity to strangers in public place.

d) Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.

e) Always use latest and update antivirus software to guard against virus attacks.

f) Always keep back up volumes so that one may not suffer data loss due to virus.

g) Never send your credit card number to any site that is not secured, to guard against frauds.

h) It is better to use a security program that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.

i) Website owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.

j) Use of firewalls may be beneficial.

5. References

Adeniran, A. I. (2008). The Internet and emergence of Yahooboys sub-culture in Nigeria. *International Journal of Cyber Criminology*, 2(2), 368-381.

Ayofe, A. N., & Oluwaseyi, O. (2009). Towards ameliorating cybercrime and cybersecurity. *International Journal of Computer Science and Information Security*, 3(1), 1-11.

Balogun, V. F., &Obe, O. O. (2010). E-Crime in Nigeria: Trends, Tricks, and Treatment. *The Pacific Journal of Science and Technology*, 11(1), 343-355.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., &Chon, S. (2014). An analysis of the nature of groups engaged in cybercrime. *International Journal of Cyber Criminology*, 8(1), 1-20.

Dashora, K. (2011). Cybercrime in the society: Problems and preventions. *Journal of Alternative Perspectives in the Social Sciences*, 3(1), 240-259.

Ehimen, O. R., &Bola, A. (2010). Cybercrime in Nigeria. *Business Intelligence Journal*, 3(1), 93-98.

Hassan, A. B., Lass, F. D. & Makinde, J. (2012). Cybercrime in Nigeria: causes, effects and the way out. *ARPN Journal of Science and Technology*, 2(7), 626-631.

Internet Crime Report, Internet Crime Complaint Center, 2011 www.ic3.gov/media/annualreport/2010_IC3Report.pdf

Le, L. B., Lau, V., Jorswieck, E., Dao, N. D., Haghighat, A., Kim, D. I., & Le-Ngoc, T. (2015). Enabling 5G mobile wireless technologies.

Mitra, R. N., & Agrawal, D. P. (2015). 5G mobile technology: A survey. *ICT Express*, *1*(3), 132-137.

Moses-Òkè. (2012) Cyber capacity without cyber security: A case study of Nigeria's National Policy for Information Technology (NPFIT). *The Journal of Philosophy, Science & Law*, 12(1), 1-14.

Okeshola, F. B., & Adeta, A. K. (2013). The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research*, 3(9), 98-114.

Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*,6(3), 116-125.

Olusola, M., Samson, O., Semiu, A., & Yinka, A. (2013). Impact of cybercrimes on Nigerian economy. *The International Journal of Engineering and Sciences*, 2(4), 47.

Reddy, M. H., Jaswanth, S., & Pramod, N. V. (2016). Evolution of mobile networks: from 1G TO 4G. *Adv. Res. Electr. Electron. Eng*, *3*(4), 307-310.

Sharma, P. (2013). Evolution of mobile wireless communication networks-1G to 5G as well as future prospective of next generation communication network. *International Journal of Computer Science and Mobile Computing*, *2*(8), 47-53.

Terrill, W. A. (2012). Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power. *Parameters*, 43(3), 146-149.