International Journal of Basic Science and Technology
July, Volume 11, Number 2, Pages 197 - 203 http://www.ijbst.fuotuoke.edu.ng/ 197
https://doi.org/10.5281/zenodo.16729087 **ISSN 2488-86**

Cybercrime: A Threat to National Security in Nigeria

Godslight, Thomas Sese
Department of Computer Science and Informatics (Cyber Security Programme)
Federal University Otuoke, Bayelsa State, Nigeria

Article Information

Article # 100280
Received: 20th March. 2025
1st Revision 5th June. 2025
2nd Revision:16th June 2025
Acceptance:29th June 2025
Available online:
2nd August 2025.

Keywords
National Security
Cybercrime
Threat

Abstract

It is no news in Nigeria that cybercrime has become a smart and fast means to an end without considering the dangers it exposes its targeted victims and the country at large. It has consistently exhibited an upward movement, especially in the area of scams, website cloning, phishing, fraudulent electronic mails, cyber harassment, data breaches, online deception, Automated Teller Machine Fraud, employment scams, among others. This menace, which is spreading like wildfire predominantly among youths in Nigeria, has eventually become a threat to national security. This study aims to identify the causes of cybercrime and recommend solutions to ensure a safe cyber ecosystem. Thus, the essence of this paper is to bring to bear how cybercrime constitutes a threat to national security. A qualitative research method was employed utilizing document and content analysis. Data collection was from secondary data sources. Findings reveal that the Nigerian population has been on a steady increase from 2020 to 2024, with a minimum rate of 2.10% in 2024 and a progressive increase of 3.8% in the urban population between 2020 and 2024. This study further reveals that the unemployment rate increased from 4.1 in Q1 2023 to 5.0 in Q3 2023. Youth unemployment increased from 6.9% in Q1 2023 to 8.6% in Q3 2023. Urban unemployment moved from 5.4 in Q1 to 6.0 in Q3 of 2023. Findings also reveal that Nigeria is the 5th country in the world with the highest cybercrime incidents, with an impact rate of 8.25, with professionalism rate of 6.49 and 52.17% in scams. Recommendations include strict compliance with data protection laws, reducing unemployment, increasing cybersecurity manpower, among others.

***Corresponding Author:** Godslight, T.S.; sesegt@fuotuoke.edu.ng

Introduction

Crime committed via the internet or with the aid of an electronic device has become a menace. The essence of computer systems, computer peripherals, the World Wide Web (WWW), the International network (Internet, and the advancement of Artificial Intelligence (AI) to enable the swift and smooth running of our day-to-day activities has been misinterpreted, misused and weaponised. Gradually defeating its genuine intentions and proper use for the benefit of mankind. However, the advancement of computing science, which has rapidly become part and parcel of human existence with high demand, dynamic changes in human needs, has also allowed government and nongovernment actors, as well as individuals, to exploit vulnerabilities for gains. Thus, putting millions of lives in harm's way. Some of these vulnerabilities include, but are not limited to, outdated software, weak passwords, unpatched software, no or inadequate security policies, deficient cybersecurity professionals, weak implementation of the national cybersecurity strategy, deficient skilled manpower, no or low enlightenment coverage, illiteracy, inherent human empathetic and sympathetic nature, etc. However, the intent of exploiting these vulnerabilities to cause harm, damage, destruction or danger is thus considered a threat. Thus, the execution of these threats becomes a crime.

Considering the levels of threat, the advancement of computing science has made us realise and understand that in the world today, cybercrime is now considered a potential threat to national security. It is considered a threat because it poses a danger at the individual level, the cooperate groups which include organisations, institutions, agencies and the nation state. Some of the identified trending and emerging crimes which has become a threat to Nigeria's eco-system and its citizens includes fraudulent electronic mails, identity theft, data breaches, cyber harassment, Automated Teller Machine (ATM) fraud, phishing, cyber stalking/cyber bulling, e-mail spoofing, sim swap, cyber pornography, cyber-defamation, social engineering, DOS/DDOS Attacks, cyber-terrorism and hacktivism amongst others. (Cybersecurity Trends and Predictions, 2024).

https://doi.org/10.5281/zenodo.16729087 ISSN 2488-86

According to the National Bureau of Statistics Q1 report on telecoms data (2024), it is eliciting that despite the current cybersecurity challenges faced in Nigeria today, the number of internet users isn't decreasing. This is a result of the positive innovations in technological advancement in computer science and the opportunities therein. Cutting across all sectors of life including but not limited to the banking industry, e-commerce, education, smart home technology, the movie industry, engineering, the health sector, mass communication, agriculture, creative arts just to mention but a few. Nevertheless, the increasing rate of internet access is warranted by the general acceptance of mobile electronic devices such as mini frame computers, connectors, notebook laptops, smartphones and smart wrist watches etc, which form a major means of internet access.

With the irreversible increasing population rate in Nigeria as opined by the "Worldometer", (2024) and the dynamic nature of computing technologies, have an irreversible growing impact on Nigerian youths who access the cyber space using mobile electronic gadgets for diverse purposes such as communication, online shopping, flight ticket booking, online taxi bookings, funds transfer, online food vendors, airtime recharge amongst others.

As Nigerians, especially the youths, swiftly adjust to the dynamic but progressive changes in computing technologies by engaging themselves with internet activities, contributing to the development of a cyber-driven society, it also forms a major source of threat as vulnerabilities are exploited by individuals, state and non-state actors.

Cybercrime

According to Media Defence (2020), cybercrime refers to a crime that is committed within the ambit of cyberspace or the internet. This can cover a wide range of activities, including cyber warfare, cyber terrorism, industrial espionage, hacktivism, unauthorised access to computer systems and networks, content-related offences, data theft/manipulation, online fraud, identity theft and cyberstalking, among others. Cybercrime involves unlawful actions executed using electronic devices and the internet to inflict harm and or damage. Aminu (2023) opined that cybercrime is a social issue within Nigeria, encompassing a range of illicit activities conducted using computers or networks. Thus, cybercrime is the process of gaining unauthorised access to systems and networks with the intent to spy, modify, destroy, or steal classified data/information for personal gain or gratification.

However, cybercrime is considered a subset of computer or digital crime. In other words, every crime committed within cyberspace is a digital or computer crime due to the use of an electronic device. On the other hand, not all computer or digital crime is considered cybercrime. This is so because any crime committed outside the ambit of cyberspace should not be considered cybercrime; rather, such crimes should be referred to as computer or digital crimes. For instance, having unauthorised access to a standalone PC is a computer crime. Extracting, editing or modifying restricted files from electronic devices is also a computer or digital crime. These can be done without having access to the internet. Thus, for the fact that an electronic device is involved, it is a computer crime.

Prevalent Cybercrimes in Nigeria

Online Deformation: Online character assassination is gradually becoming a very lucrative venture in Nigeria. Ranging from the political scene, to education, religion and even in content creation within the entertainment industry, etc. Some even go as far as uploading sexual content for personal gain. Such actions inflict unforgettable scars on the victims. Some of which may be for extortion, blackmail or humiliation. Thus, leaving targeted victims hopeless and helpless as justice eludes them against the perpetrators.

Cyberbullying: Another rampant cybercrime within Nigeria's cyberspace is cyberbullying. This occurs when disgruntled individuals, state and non-state actors, send direct or indirect threats to their targeted victims. It is also worth noting that the crime of cyberbullying, which is the sending of intimidating or threatening messages, is common among juveniles and youths (Media Defence, 2020). It is a repeated behaviour aimed at scaring, angering or shaming those who are targeted. Instances include spreading lies, posting nude photos of their victims, sending messages of threats and impersonating their target by sending mean messages to others on their behalf.

Website Cloning: This has to do with the development of a twin site having similar features and entities. With similar features and entities, such fraudulent sites thus appear very real in the sight of ignorant internet users. Hence, internet users with little or no navigation skills end up trusting the fraudulent site for the real ones, thereby ignorantly providing personal and confidential information to swindlers. Instances include desperate young graduates seeking jobs online, individuals seeking government and organisations' grants, undergraduate students seeking admission into higher institutions and online purchase of goods, etc. Cybercriminals often employ proxy

https://doi.org/10.5281/zenodo.16729087 ISSN 2488-86

services to hide IP addresses, carry out attacks across national boundaries, and collaborate with partners with superficial measures not capturing the true geographical distribution of these offenders (Bruce et al, 2024).

ATM Fraud: This type of crime often occurs as a result of misplaced, stolen or forgotten ATM cards that eventually fall into the hands of script kiddies. Such cards are mostly used to make online purchases if the perpetrator finds it difficult to have access to the ATM PIN to avoid being traced. ATM fraud can also occur when close friends, classmates, relatives, colleagues, or even a separated spouse have access to ATM Card Credentials. These credentials are thus used by the perpetrator to pose as the legitimate owner to authorise transactions. However, some of these credentials may be as a result of known pins and unchanged phone patterns, understudied by the perpetrator. This action might cause the victim financial losses, depression, closure of petty and small-scale businesses, it can lead to the arrest of the victim if the money involved is obtained from individual daily or weekly contributions called "Osusu" or "Akawo", mostly expressed in the southern Nigerian parlance. Thus, in a very severe situation, the victim might attempt or commit suicide. Imagine a nation state whose suicide rate is attributed to cybercrime. Of course, it will gradually become a national security concern.

Phishing: Phishing is a form of social engineering and a scam where attackers deceive people into revealing sensitive information. It is also referred to as a cyber threat which attempts to gain sensitive information like passwords, usernames and other details for malicious reasons. It is an email fraud where the perpetrator sends a legitimate-looking email and attempts to gain personal information (Nilesh *Ed*. 2021). These messages typically redirect to a fake login page where the user is prompted to enter their login credentials.

Deep-fake: Deep-fake technology involves editing audio and video to mimic realistic but fake content. It is employed for social engineering attacks, impersonation, and spreading fake information. Some of such content is usually AI-generated or popularity, financial gains, blackmail, hacktivism or self-gratification. As this crime gathers momentum, individuals, corporate organisations and the nation state must ensure the application of basic security access control protocols on all electronic devices to reduce the level of damage.

Insider Threat: It is no news that Nigerians are facing a high inflation rate in goods and services. This has eventually led to rising economic challenges across the nation. Oluwafemi *et al*. (2023) predicted that Nigeria will face an upsurge in insider threats in 2024. They further stated that amid these economic hardships, cybercrime will become an increasingly attractive option, offering substantial `illegal earnings. Thus, increasing both poverty and death rate as a result of the survival of the fittest syndrome persists. Several instances of insider fraud include executive and junior-level involvement. Employees might be tempted to sell sensitive personal information of their clients to cybercriminals. In the worst-case scenario, they might even collaborate with cybercriminals as a viable way to meet their family's demands based on the current economic realities in the country.

Employment Scams: According to Oluwafemi *et al*. (2023), Nigeria will witness a surge in employment scams, a trend that has been prevalent in the country. This is a result of population growth, immigration from rural to urban cities and the huge number of graduates produced by the Nigerian universities yearly without jobs. Oluwafemi et al (2023), also opined that the last quarter of 2023 saw the Nigerian military issuing warnings against fake online job recruiters. Cybercriminals scammed their targeted victims by advertising fraudulent recruitment exercises on clone websites. This scam is attributed to Nigeria's inflation rate of goods and services. Thereby, making job seekers to scout for financial opportunities within cyberspace notwithstanding the dangers ahead.

Resultant Perils of Cybercrime: In this study, the resultant effects of cybercrime are categorised into three major parts, which are viz: Effects on family members, Effects on corporate bodies (Organisations, Institutions and Agencies), and Effects on the nation state.

Effect on Family Members: Cybercrime can result in the theft of personal information, including bank account details, Bank Verification Number (BVN), National Identification Number (NIN), and credit card information. This stolen data is often used by cybercriminals to commit identity theft and financial fraud, by authorising transactions from first, second and third-tier bank accounts. Individuals may also suffer greatly from the loss of personal data due to data breaches. Consequently, cybercrime poses psychological effects on victims, which can lead to mental irritations, depression, frustration and emotional trauma. In situations where justice eludes the victim(s), suicide or a suicide attempt might be

https://doi.org/10.5281/zenodo.16729087 ISSN 2488-86

considered. Thus, it hurts the victim(s)'s general well-being.

Effects on Corporate Bodies Organisation/Institutions: Cybercrime against cooperate bodies in Nigeria can be very fatal and, in some cases, irreversible. It has the capacity of damaging the image of the cooperate body, soil reputation, weaken client and public trust and cooperate litigation. This will eventually give room for public perception of inadequacies in security policies and their weak implementation style. Intending investors, as a result of public perception against such cooperate bodies, withdraw their investment plans, causing great financial losses. Substantive financial losses might further result in the retrenchments of workers, an increase in unemployment and poverty rates.

Effects on Our Nation State:
Cybercrimes committed against the Nigerian government system, such as unauthorised access to classified information, constitute a significant threat to national security. Such information can be used against the Nigerian state as perpetrators exploit more vulnerabilities. These exploited vulnerabilities will eventually tend towards the disruption of government operations, such as the manipulation of election results, which will in turn affect citizens' opinions. Cybercriminals can also spread and incite their citizens through propaganda against the government, causing social unrest and unnecessary security alerts. Cybercrime can also warrant political instability and threaten international relations.

Causative Theory: Theories of crime causation attempt to explain why individuals or groups engage in criminal activities. This paper employed the Routine Activity Theory as it best explains how cybercrime constitutes a threat to national security. Routine Activity Theory (RAT) is an environmental place-based explanation of crime which emphasises its relation to space and time. Cohen and Felson (1979), in a bid to provide an explanation for why crime occurs, propounded this theory with its main assumption that crime occurs when three elements converge in time and space. The presence of all three elements increases the likelihood of criminality, while the absence of these elements might reduce the chances of criminality. According to Cohen and Felson (1979), these three elements are a motivated offender, a suitable target and a lack of capable guardianship.

Motivated Offender: The potential offender gets motivated by the presence of suitable target(s). in cybercrime, the motivated offenders are scammers, identity thieves, hackers and other criminally minded individuals or groups who are driven by financial gains, political motives or revenge. These criminal-minded individuals often have technical skills and access to anonymising tools like a Virtual Private Network (VPN) and the dark web. An instance is a hacker using phishing emails to steal banking credentials.

Suitable Target: A suitable target can be a person, an object, or a place that is attractive to an offender. Suitable targets are things that provide instant profit or gratification to the offenders. These offenders exploit vulnerabilities found in systems and networks or as a result of human error. In cybercrime, suitable targets are often individuals with weak passwords, unsecured systems or networks, organisations with poor cybersecurity practices, and users of social media platforms, sharing sensitive personal information that are sensitive. An instance is someone who clicks on a fake email. Cohen and Felson (1979) identified value, inertia, visibility and accessibility as the four factors that affect a target's suitability.

Absence of Capable Guardian:
Cybercrime activities increase without the presence of capable guardianship. In cybersecurity, guardianship includes antivirus software, firewalls, multifactor authentication, cybersecurity policies and cybersecurity awareness and enlightenment. When these guardianships become weak or absent, cybercrime increases. Thus, the increase becomes a threat to national security. For instance, an agency without endpoint security software becomes a ransomware target.

Materials and Methods

Study Area: This study is centred within the Federal Republic of Nigeria, with an estimated population of 232,679,478. Thus, the most populous black nation in the world.

Research Method: A Qualitative research method was employed, utilising document and content analysis, which focuses on understanding the meaning and context behind human experiences through in-depth interviews and observations to produce descriptive and rich data. The criteria considered in the selection of the secondary data include the purpose and scope of the paper, the timeliness of the data, accuracy/reliability of the data, bias/objectivity, relevance and applicability of the data.

Data Source: The data used in this study were collated from secondary data sources and expert interviews to complement the secondary data.

https://doi.org/10.5281/zenodo.16729087 ISSN 2488-86

Results and Discussion

The "Giant of Africa", as Nigeria is often called, has been established to be the 6th most populous country in the world, with a percentage increase range between 2.10% to 2.15% from 2020 to 2024, with an average age of 17.9 years in 2024 (Worldometer, 2024)

Thus, having a yearly estimated population increase of over four million people (4,000,000), Nigeria has retained its position over the last four years. The consistent progressive increase in population has also affected the population of urban dwellers steadily, as citizens migrate from rural settlements seeking greener pastures due to economic realities and access to social amenities. However, the immigration from rural to urban areas, which is conditioned by the current economic reality, has eventually triggered the mindset of survival of the fittest syndrome amongst Nigerian youths. Thus, giving rise to cybercrime, which is considered the fattest means to financial people as their victims are placed in harm's way as a result of their actions.

Table 1: Population of Nigeria from 2020 to 2024

Year	Population	Yearly % Change	Yearly Change	Median Age	Urban Pop %	Urban Population	Nigeria Global Rank
2024	232,679,478	2.10 %	4,796,533	17.9	53.9 %	125,447,884	6
2023	227,882,945	2.12 %	4,732,049	17.8	53.0 %	120,696,717	6
2022	223,150,896	2.11 %	4,621,610	17.6	52.0 %	116,057,853	6
2020	213,996,181	2.15 %	4,510,540	17.2	50.1 %	107,112,526	6

Source: Worldometer (2024)

Table 2 shows an increase in the youth unemployment rate difference of 1.7% between Q1 and Q3 of 2023. It also indicates an increase of 0.6% of the urban unemployment rate and a 1.1% increase in the rural unemployment rate between Q1 and Q3 of the same year. Although there isn't any significant progression of informal employment in 2023.

However, a significant progressive increase rate of the 5.0% unemployment rate in Q3 of 2023 is a clear indication why cybercrime is gradually becoming a potent threat to national security. The Nigerian government has to take proactive steps to curb this menace before it gets to the level of irreversible economic and system downtimes, social unrest, political instability and weak international relations.

Table 2: Key Labour Market Indicators.

Key Labour Market Indicator	Q1 2023	Q2 2023	Q3 2023
Unemployment Rate	4.1	4.2	5.0
Youth Unemployment Rate	6.9	7.2	8.6
Urban Unemployment Rate	5.4	5.9	6.0
Rural Unemployment Rate	2.9	2.5	4.0
Informal Employment	92.6	92.7	92.3

Source: Nigeria Labour Force Statistics Report (2024)

Table 3 ranks Nigeria the 5th country in the world with the highest cybercrime incidents, with an impact rate of 8.25. Nigeria, having 52.17% in the scam column, automatically ranks as the highest country with scams in the world. However, Nigeria has been the country with the highest scam rate in the world can be attributed to a lot of factors, including but not limited to high unemployment rate, high inflation rate of goods and services, low-income wages, low access to social amenities, inadequate price control mechanisms and inadequate cyber security professionals, amongst others.

https://doi.org/10.5281/zenodo.16729087 ISSN 2488-86

Table 3: Cybercrime top 15 countries.

Rank	Country	I	P	TS	WCI Score (%)	Tech (%)	Attacks (%)	Data (%)	Scams (%)	Cash (%)
1	Russia	8.96	8.81	8.73	58.39	82.17	81.34	65.18	21.70	41.56
2	Ukraine	8.37	8.29	8.24	36.44	52.97	50.76	36.01	11.20	31.27
3	China	8.22	7.70	7.81	27.86	40.22	24.24	34.89	15.83	24.13
4	USA	7.99	7.21	7.21	25.01	27.64	17.68	30.36	22.72	26.63
5	Nigeria	8.25	6.49	5.80	21.28	7.93	8.41	23.04	52.17	14.86
6	Romania	7.12	7.04	7.15	14.83	17.89	9.17	22.50	13.15	11.49
7	N. Korea	7.91	7.23	7.83	10.61	8.66	25.33	13.01	2.17	3.88
8	UK	7.86	7.21	6.75	9.01	5.04	4.75	5.80	7.86	21.63
9	Brazil	6.90	6.35	6.32	8.93	13.70	8.77	10.29	7.28	4.64
10	India	7.90	6.60	6.65	6.13	4.46	3.62	6.81	12.75	3.01
11	Iran	6.88	6.45	6.64	4.78	8.62	10.00	3.59	0.94	0.72
12	Belarus	6.84	7.20	7.32	3.87	11.92	5.58	1.85	--	--
13	Ghana	8.57	6.83	6.09	3.58	1.23	0.76	2.97	10.36	2.57
14	S. Africa	6.95	5.35	5.50	2.58	1.20	0.65	0.58	7.17	3.30
15	Moldova	7.38	7.19	7.56	2.57	6.70	0.98	2.43	0.83	1.88

Source: World Cybercrime Index (2024).
I = Impact; P = Professionalism; TS = Technical skill, Tech = Technical products/services, Attacks = Attacks and extortion, Data = Data/identity theft, Cash = Cashing out and money laundering. I, P, and TS are scored out of 10

Conclusion: Since the advancement of technology has become part and parcel of human existence and cannot be thrown overboard, vulnerabilities will always be exploited by state and non-state actors for personal gains, gratification, or to express superiority. However, the intent behind such actions, any unauthorised access, attempt or identified potential to cause harm to Nigeria's information and communications systems, networks and infrastructure to destabilise economic growth, social unrest and political instability that tends to weaken international relations shall be considered a threat to national security.

Thus, to ensure a safe cyber ecosystem in Nigeria, the existing cybercrime laws should be strengthened by putting in place a rigid implementation mechanism, which will in turn deter others who may likely have the intent to commit cyber or computer-related crimes. Furthermore, data protection laws should be strengthened to ensure that only authorised security-cleared individuals have access to sensitive information at all levels.

Thus, to adapt to these changes, there is a need for strengthened cybersecurity laws in Nigeria to strike the much-needed balance in Cybersecurity. Also, Nigeria's cybersecurity landscape is characterised by a need for enhanced legal and regulatory frameworks, a growing recognition of the importance of cybersecurity, and the presence of general and sector-specific legislation to address cyber threats and data protection.

Recommendations

To downplay the actions of cyber criminals from being a threat to national security, the Nigerian government should:

1. Enlighten the citizens on the dangers cybercrimes can bring to bear.
2. Ensure strict compliance with data protection laws and prosecute offenders according to the provisions of the law.
3. Reduce the unemployment rate in the country through a government-private partnership.
4. Monitor the mode and degree of implementation of data protection policies and frameworks by defined business organisations and cooperating bodies as enshrined in the Data Protection Act.
5. Adapt to the dynamic changes in the advancement of cybersecurity technologies by investing in technological infrastructure.
6. Rapidly increase the manpower of cybersecurity professionals in the country.
7. Establish an independent paramilitary agency of diverse cybersecurity expertise in all 36 states with the legal powers to gather credible intelligence, and investigate, arrest, detain and prosecute offenders according to the provisions of the law.
8. Encourage and support the development of local technologies in the fight against cybercrime.

https://doi.org/10.5281/zenodo.16729087 ISSN 2488-86

9. Establish regional cybercrime research centers to identify futuristic potential cybersecurity threats.
10. Develop a rich, futuristic content-based curriculum that the Ministry of Education will implement in all Nigerian universities.
11. Create room for collaboration between the government, the private sector, and international organisations.

References

Aminu, M. A. (2023). The Overview of Cybercrime and Cyber Security in Nigeria and Its Future Trends. *Research Square*. https://doi.org/10.21203/rs.3.rs-3307532/v2

Bruce, M., Lusthaus, J., Kashyap, R., Phair, N. and Varese, F. (2024). Mapping the Global Geography of Cybercrime with the World Cybercrime Index. *PLoSONE 19(4): e0297312*. https://doi.org/10.1371/journal.pone.0297312.

Cybersecurity Trends and Predictions (2024). *Computer Emergency Response Team (Mauritius) CERT-MU*. https://cert-mugovmu.org.

Cohen, L. E. and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44(4), 588–608*.

Nilesh K. M. (Ed. 2021). Cyberattacks and Counter Measures. User Perspective. *Dr. Babasaheb Ambedkar Open University*. https://baou.edu.in.

Nigeria Labour Force Statistics Report Q3 2023 (2024, February). *National Bureau of statistics.* https://www.nigerianstat.gov.ng

Oluwafemi, O., John O., Hamzat L., Olajumoke O. and Jonathan A., (2023). National Cyber Threat Forecast 2024. *Cyber Security Experts Association of Nigeria (CSEAN)*. https://csean.org.ng.

Summary Modules on Litigating Digital Rights and Freedom of Expression Online in Sub – Saharan Africa. (2020). Module 7 – Cybercrimes. *Media Defence* https://www.mediadefence.org.

Telecoms Data: Active Voice and Internet, Porting and Tariff Information (2024, June). *National Bureau of Statistics*. https://www.nigerianstat.gov.ng.

Worldometer (2024). https://www.worldometers.info