Management Analytics and Social Insights

www.masi.reapress.com

Manag. Anal. Soc. Insights. Vol. 2, No. 2 (2025) 95–107.

Paper Type: Original Article

Effects of Cybercrime on National Development: A Literature Review

Salvation Ifechukwude Atalor[1], **Olutayo Sunday Fakunle**[2,]*

[1] Departmant of Computer Science, Prairie View A&M University, Texas, USA; salvationatalor@gmail.com.

[2] Department of Sociology, Redeemers's University, Ede, Osun State, Nigeria; fakunles@run.edu.ng.

Citation:

Received: 12 January 2025 *Revised: 14 March 2025* *Accepted: 26 April 2025*	Atalor, S. I., Fakunle, O. S. (2025). Effects of cybercrime on national development: A literature review. *Management analytics and social insights,* 2(2), 95-107.

Abstract

This study examined the effect of cybercrime on national development. The study was conducted in Nigeria because of the increasing trend of cybercrime worldwide. Several works of literature in the subject matter were examined. The study found that cybercrime undermines investor trust in the economy, injures the reputation of Nigerians abroad, and results in security risk. Cybercrime frequently results in the loss of intellectual property and retards the sustainable growth of the country. It hinders competitive advantages and the company's brand. It was concluded that cybercrime negatively affects people, perception, government, and society. As a result, the study suggests that the government of Nigeria creates frequent sensitization programs and campaigns against cybercrime and its effects in Nigeria and that both private and government sectors give young people access to employment opportunities. The government should also pass legislation that could effectively punish those involved in cybercrimes. The agency saddled with tackling cybercrime Economic and Financial Crimes Commission (EFCC) should be independent, and the staff should be incorruptible. Finally, the government should create awareness of individual security and safety in online-related matters.

Keywords: Cybercrime, Implications, National development, Youths.

1 | Introduction

Recently, Information and Communication Technology (ICT) systems are used in almost every aspect of a person's life, including homes, businesses, governments, and associations. Humans rely extensively on ICT to do their daily tasks [1]. The ICT system is beneficial for convenience, effectiveness, and enjoyment; however, it also serves as a significant engine for innovation, economic expansion, and development [2]. The tech-driven age of the 21st century is transforming the globe into an information society with extensive

Corresponding Author: fakunles@run.edu.ng

https://doi.org/10.22105/masi.v2i2.68

information interchange in cyberspace, and it is progressively growing more dynamic and complex. Since around three decades ago, dishonest computer users persisted using the device to perpetrate various crimes.

Technological advancements have brought about exciting new advantages and possibilities but have also made people more vulnerable to crime [3]. The incidence of cybercrime has surged in a way never seen before. Every day, cybercrime is a complex and dynamic act. The technology is now so sophisticated that it may be used to carry out murder and other crimes in other domains without ever leaving the current geographic area. The abuse or misuse of digital resources in a cyber environment via the internet is known as cybercrime in networks and computer systems.

Unauthorized computer systems and data interception are what it is all about: Gaining personal information or manipulating it for one's gain. In the realm of computers and the internet, cybercrime occurs. Cybercrime is any act compromising the availability, confidentiality, and integrity of data and computer system networks, among other things. Hacking, theft/cloning of customer bank cards, fraudulent transfers or withdrawals of customer funds, hacking of banking software for the transfer of funds, cloning of bank/business websites to deceive customers, and sending of emails or texts requesting assistance or personal information from unsuspecting individuals are the most common cybercrimes in Nigeria.

Software piracy, identity theft, denial of service attacks, credit card and Automated Teller Machine (ATM) card fraud, web-based (online banking) scams, Spread of viruses, phishing, cyber plagiarism, cyberterrorism, spam, malware, and cyberstalking are examples. Technology is causing many societal changes that the globe is now going through. Thanks to technology, communicating via phone (GSM), computer, internet, fax, email, and other means is now simple and quick. Cybercrime is one of the problems associated with these advances.

The utilization of computer networks and the high-tech environment of the twenty-first century have increased crime rates. Since cybercrimes are international in scope, it is difficult for governments to block incoming cyber threats. The location of the victims, time, and space are no longer constraints on the cybercriminals' launch times and locations of these assaults. According to Paranjape [4], cybercrime differs from most terrestrial crimes in that it is simple to learn how to commit, requires few resources compared to the potential damage caused, and can be committed in a jurisdiction without the perpetrator's physical presence. Additionally, cybercrimes are not always explicitly illegal because most national laws do not expressly forbid them [5].

Furthermore, cybercrime in contemporary world is posing a serious threat to the society even when organizations incorporate robust security technology (cyber security) such as firewalls, antivirus software, intrusion detection tools, authentication services, Personal Identification Numbers (PIN), and so on, yet cybercrime keeps on spreading. It is no longer confined to traditional juvenile hackers, as professional criminals are now exploiting the network for profit. Computer and communication systems in the world are not immune from cybercrime as it is possible that cyber-criminals can crack any and every system in the world.

Cybercrime can be against persons or property and/or against the government – state, and/or society. The nature of cybercrime is numerous, and it includes hacking, virus attacks, cyberstalking, marriage scams, cyber contra band, spam, telecoms fraud, pedophiles, cybertrespass, cracking of satellite or TV decoding devices, convincing people to buy unwanted software via the net (scareware), using of the web to spread lies (fake news), hoaxes and urban myths and so on. The growth of international data communication, particularly the internet, has made cybercrime more common.

Cooperation across national borders to solve and prosecute cybercrime-related acts is complex, even with international pressure. The magnitude of cybercrime in many nations threatens the capacity of many countries to participate in the digital economy; hence, countries perceived as cybercrime havens risk having their electronic messages blocked by the network.

In Nigeria, cybercrime ballooned after a few years and has become the fastest-growing country for cell phone and internet use. Thus, continuous research becomes imperative considering the impact and dimensions of cybercrime nationally and globally. Cybercrime impacts the economy and the lives of the people in the society. Information systems and businesses have been compromised, and the economic impacts have been devastating. Cybercrime has brought misery to human beings, as it facilitates the easier commission of crimes like terrorism, transnational economic and financial crimes, as well as political and economic espionage that are perpetrated within and across countries.

Cybercrime seriously threatens national security, socioeconomic development, political stability, and fundamental human rights. The effects of cybercrime on Nigeria's natural economic development and sustainability cannot be over-emphasized. Various crimes are perpetrated by criminals using computers over the internet and other devices. Criminal activities affect the national economy. Cybercrime impacts national development, as it has the propensity to negatively affect foreign direct investment and national economic development. The national economic growth and development would not be financially stable. Cybercrime significantly impacts national security and does not allow economic development and growth.

The impact of cybercrime on Nigeria's per capita income is exceptionally high. Cybercrime is taking its toll on the Nigerian national economy. With Nigeria venturing into a cashless society, small and medium enterprises are becoming reluctant to use mobile banking for fear of cybercrime, reducing sales and impacting per capita income. Cybercrime is an obstacle to several targets of Sustainable Development Goals (SDGs), such as those under goal 16, which relate to money laundering, combating the financing of terrorism, corruption, and arms trafficking the SDGs report [6]. Cybercrime threatens the nation's technological, educational, political, security, and socioeconomic growth and development [7].

2 | Concept of Cybercrime and Modern Technology

Depending on their differing viewpoints, scholars worldwide have defined cybercrime in various ways and in terms of different dimensions. As a result, the concept of cybercrime is contextual rather than having a universally accepted term. Cybercrime, on the other hand, can be defined as hacking, publishing electronic information that is not authorized, data interference, system interference, illegal interception, illegal access, and the misuse of a device for fraudulent purposes. Cybercrime also includes breaking into computers to steal or destroy information or damage computer source code. Therefore, intrusions into private and corporate data, breaches of network integrity, privacy violations, industrial espionage, software piracy, and other crimes where a computer plays a significant role in committing the crime are all considered cybercrimes.

Cybercrime is defined as the following: Denying end-user access to their hardware, software, data, or network resources; unauthorized release of information; unauthorized copying of software; unauthorized use, access, modification, and destruction of hardware, software, data, or network resources; and using or conspiring to use computer resources to obtain information or tangible property illegally [5]. The illicit compromising of information security is known as cybercrime. Cybercrime is any illegal behavior in which a computer or network is the crime's source, instrument, or location [4]. This includes fax, phone, and Very Small Aperture Transmission (VSAT) networks. Cybercrime, then, is a crime using information and communication.

Crimes done online that use a computer as a tool or a targeted victim are known as cybercrimes. Using networked computers, phones, and other ICT devices promotes any unlawful activity carried out by one or more individuals known as scammers, hackers, online fraudsters, cyber citizens, or 419ners. Mobile phones, tablets, computers, and whole networks are all targets of cybercrimes [8]. Cybercrime, as defined by Ayofe and Oluwaseyifunmitan [9], is any illegal action in which a computer or computer networks are used as a tool, a target, or a media. Therefore, any malicious act from or against a computer or network is considered a cybercrime. Cybercrime is distinct from most terrestrial crimes in the following ways:

I. Learning to commit to them is simple.

II. They need minimal resources compared to the possible harm they may inflict.

III. They can occur in a jurisdiction even if the perpetrator is not physically there.

IV. They are frequently not unlawful.

V. Anyone over a certain reasonable age can commit it [4].

Cybercrime, often known as computer crime, is any unlawful activity that attacks the security of computer systems and the data they handle and is carried out using electronic methods. Cybercrime is any crime committed in a virtual environment where information about people, things, facts, events, phenomena, or processes is represented mathematically, symbolically, or in any other manner and shared across local and international networks. From the foregoing, it is clear that cybercrime involves causing havoc with computer data or networks by interfering with, destroying, or intercepting such data or systems. According to Ayofe and Oluwaseyifunmitan [9] and Uroko [10], it entails committing crimes against computer systems or using computers to conduct crimes.

Technology not only facilitates criminal investigation but also encourages crime. Cyberterrorism, money laundering, counterfeiting, advance-free fraud, and other crimes frequently entail using contemporary technology, especially "ICT" [5], [11]. Idowu and Madaki [5] emphasized that individuals are exposed to new forms of crime, or "cybercrime," as a result of the advancements in information technology and the consequent use of the technology by Nigerian banks and others in conducting business and transactions.

Modern technology has also eliminated geographical restrictions on crime, increased anonymity, and improved the criminals' ability to evade discovery. With the advent of contemporary technology, cybercriminals can operate outside conventional boundaries and use it to expand into new regions. Equally significant, the notion of a geographical barrier that no longer constitutes a danger to hackers raises other issues, including the necessity for unified cyber laws, the threat of national boundaries, and difficulties facing the national government and law enforcement.

3 | Cybercrime and National Development

Ibrahim [12] claims that ICT has a well-established and prominent function in all human endeavors. Through the use of electronics and the internet, ICT has helped to integrate the world's economy. Everyone, even criminals, may now access the electronic market. According to Hassan et al. [13], some consequences of cybercrime include the loss of an organization's competitive edge, waste of time and poor financial development, delayed production time and increased overhead costs and damage to a country's reputation. Loss of privacy and financial losses are two more significant consequences.

Ibrahim [12] went on to say that the effects of cybercrime on the Nigerian banking system and economy undoubtedly led to endless potential for Nigerian banking institutions, especially in internet and financial software. For both depositors and banking institutions, it made transactions easier and lower costs. However, it also brought unique threats, such as cybercrimes, significantly affecting the economy and business. Any country's inhabitants face serious dangers. Without question, cybercrime is harming Nigeria's reputation, which continues to be a significant cause of shame for the nation. Many people avoid using ICT because they are afraid of cybercrime.

This negatively impacts the well-being of investors and citizens. Cybercriminals' actions undermine trust in a country's financial system. Both visitors and potential investors are terrified, and the public's perception is damaged. In today's global economy, citizens risk reputational damage; a country cannot afford to be linked to cybercrime and have its financial system's brand damaged. When every person is seen as a potential scammer, it becomes difficult for them to communicate socially with the rest of the world. Since foreign investments find it challenging to enter the economy, the perceived decline in trust may also impact the nation's developmental growth.

As a result, the country is viewed as an economic outcast. The economy may suffer significantly from the lack of trust in the financial industry brought on by cybercrime. It is common knowledge that a strong financial system is essential to a thriving economy. Typically, the goal of cyberattacks is to make money. Businesses, people, banks, and other financial institutions all suffer losses due to these actions [12].

4 | Nature and Types of Cybercrime

According to James [14], cybercrimes have existed since the advent of the abacus because individuals misuse the technology. According to Shinder [15], linking the crime's inception to the first computer network is safe. In the modern world, cybercrime is a significant threat to society. "It is a new breed of white-collar offenses," according to Siegel [16].

Kudi Dukk [17] asserts that the dangerous environment changes as the internet becomes more widely available and more services depend on it for day-to-day operations. In Nigeria, cybercrime has emerged as a primary means of financial theft and corporate espionage. Nigerians are recognized both at home and abroad to be widespread perpetrators of cybercrimes. Numerous sectors of Nigeria have benefited from the Internet's contribution to the nation's growth. Nonetheless, the impact of cybercrimes is a problem for industries including banking, e-commerce, and education.

According to Golubev [18], the Internet is a worldwide network that connects millions of computers across several nations and provides a wealth of information exchange and acquisition options. However, because of economic considerations, it is currently being utilized for illegal purposes. The globe has become a global village due to internet connections, giving the impression that everyone is in the exact location at the same time. Although the Internet has facilitated faster and simpler communication, many transactions are completed at lightning speed. According to Oyewole and Obeta [19], the Internet is the global network of computers that connects people, giving humanity access to countless options.

Ehimen and Bola [20] claim that the Internet has increased commercial prospects and promoted geometric growth while removing economic hurdles that nations have previously experienced. Given its countless benefits, one may readily agree that the Internet is crucial for national development in developing countries like Nigeria. According to Ribadu [21], website cloning, misleading representations, online purchases, and other e-commerce frauds are Nigeria's most common types of cybercrime. In economic interactions, Nigerians are essentially viewed with distrust.

As Ribadu [21] noted, cybercrime is lowering trade and investor trust in our economy, making it a real and apparent threat to national security and the prosperity of our people. The following are examples of cybercrime: Government fraud, tax evasion, financial fraud, securities fraud, insider trading, bribery, kickbacks, counterfeiting, embezzlement, mail scams, credit card fraud, bankruptcy fraud, insurance fraud, computer and internet fraud, and economic and copyright/trade secret theft. Website cloning, financial fraud, identity theft, credit card theft, cyber theft, cyber harassment, fake emails, cyber laundering, viruses, worms, and trojans are all included [22].

Additionally, there are other categories of cybercrime, including banking, e-commerce, education, communications, and social media. Nonetheless, the following are general examples of cybercrime: Bank Verification Number (BVN) scam, cybertheft/banking fraud, unauthorized access to hosts (hacking), online identity theft (phishing, bank card theft, atm scam), cyber plagiarism, software piracy (copy right theft), cyber-pornography, drug trafficking deals, software piracy (intellectual property theft), sales fraud and forged documents, Data and Airtime Time (DAT) theft from service providers, cyberstalking, password sniffing, malware, spam, scam mails, wire-tapping/illegal interception of telecommunication, mobile phone virus and cybercrime, mobile virus delivery vectors, charity funds, nigerian-prince (beneficiary of a will) scam, social-hi-jacking, cyber terrorism, logic bombs, and more [23].

The internet presents endless options for economic, social, and educational activity. However, it has brought its own distinctive risk that threatens the economy. The threat might impact numerous facets of society, endangering the nation's progress. Among these potential negative consequences are the devastation of the nation's reputation both domestically and internationally, the insecurity of life and property, the apprehension of conducting business with Nigerians, and the financial loss resulting from the significant expenditures made on the prevention and management of cybercrime [17]. Furthermore, several reasons can be adduced to the causes of these cybercrimes in general and Wuse, Abuja, Nigeria, in particular.

However, the significant causes of cybercrime among youths in Nigeria include unemployment, the quest for quick money syndrome, a corrupt society, the youths' criminal mindedness, a poor cyber-security system, uncertain punishment of cyber offenders, a rate of weak implementation of cybercrime laws, youthful exuberance (experimentation), incompetent security on personal computers, urbanization, and so on [10].

5 | Implications of Cybercrime in Nigeria

In evaluating the negative consequences of cybercrime in Nigeria, Ribadu [21] says cybercrime hurts trade, stifles the confidence of foreign investors in the national economy, and threatens security. Thus, cybercrime damages Nigeria's security and domestic economy. According to Awe [24], cybercrime in Nigeria has incurred heavy losses on the Nigerian citizenry and has created serious credibility and image problems for the Nigerian government.

The later problem of cybercrime has led many successive governments in Nigeria to sink enormous resources into trying to restore their battered image. Other negative impacts of software piracy, as cited by Siebel and House [25] and Broad [26], are damage to reputations, software compatibility problems, and lost time. Thus, the consequence of intellectual rights infringements is devastating [5].

In addition to causing financial loss, cybercrime has damaged Nigeria's reputation internationally. When doing business, Nigerians are viewed with suspicion. According to Ribadu [21], cybercrime is a real and apparent threat to our national security and the prosperity of our country, as it is lowering trade and investor trust in our economy. The majority of the major corruptions that occur in our communities daily are cybercrimes, which are carried out through mail scams, credit card fraud, bankruptcy fraud, insurance fraud, government fraud, tax evasion, financial fraud, securities fraud, insider trading, bribery, kickbacks, counterfeiting, embezzlement, embezzlement, economic and copyright/trade secret theft, and computer and internet fraud. Nonetheless, the following is a list of the repercussions of cybercrime:

5.1 | Decreases an Organization's Competitive Edge

Over the years, cybercrime has caused significant financial and bodily harm to private and public corporate organizations domestically and abroad. Globally, cybercrime has resulted in billions of dollars worth of yearly losses. These crimes can jeopardize a country's financial stability and security. A firm may suffer losses due to computer crime when hackers sell sensitive data and plans of the organization and only promote the business's ability to compete.

5.2 | Slows Production Time and Increases Overhead Costs

Computer crime lowers a company's productivity since it requires more time to act to prevent cybercrime, such as inputting additional passwords, which will impact productivity. Computer crime will raise costs because businesses need to purchase robust protection to lower the likelihood of assaults from viruses and malware.

5.3 | Defamation of Image

The high rate of cybercrime in Nigeria would damage the country's catchphrase, "good people, great nation," and the outside community would see both sides of the issue.

5.4 | Intellectual Property Losses

Economic espionage, or the theft of intellectual property and business-confidential information, is the most significant area for loss. In part, this is because cyber spying is not a zero-sum game; stolen data is not truly lost; spies can take a company's product plans, research findings, and customer lists today, and the company may not even be aware that it no longer has control over them tomorrow.

5.5 | Business Confidential Information

There is a blurry distinction between IP and business confidential information. Business confidential information can include "know-how" or trade secrets. The costs of losing these categories are comparable to those of intellectual property. We distinguish between IP - information that makes it simpler to build a rival product and business confidential information – information that offers an edge in commercial negotiations or in formulating competing business strategies. There is no delay in making money from stolen secret company knowledge, even if it can take years for the stolen intellectual property to appear in a rival product. The buyer can immediately exploit intelligence on oil exploration, delicate commercial negotiations, or even insider stock trading. The harm to specific businesses might be severe.

5.6 | Reputational Damage

Although businesses worry about reputational harm, much research hasn't been done to measure it. Following public disclosure of their hacking, companies experience a decrease in their value, typically manifested as a decline in stock prices. These losses can be significant - ranging from 1% to 5% - but do not appear permanent. Usually, stock prices bounce back by the next quarter. Any effort to include these stock price swings into a loss computation would be distorted. Observing whether these changes are due to new SEC rules that mandate that businesses disclose significant hacking occurrences would be intriguing. This might help shareholders better determine whether intrusions are economically meaningful.

5.7 | Increased Security and Opportunity Cost

Some studies have shown that costs associated with cyber espionage and cybercrime must also be considered. According to one estimate, governments and businesses spend most of their IT budgets on security. When calculating the cost of malicious cyber activity, opportunity costs such as missed opportunities or lost benefits that would have been available for activities in cyberspace must be considered. One example of an opportunity cost is the additional money spent on cyber security that would not be necessary in a more secure environment. Other examples include lost sales, decreased productivity, or deciding to avoid the Internet for specific purposes.

5.8 | Time Wastage and Slows Financial Growth

Wastage of time is another problem because many IT personnel may spend a lot of time handling and rectifying harmful incidents that computer criminals may cause. The time spent should have earned a profit for the organization. One odd issue is that when a hacker breaks into a business and takes private information, such as customer credit cards and other private data, the people who trust the business lose faith in it because businesses may hold private information, such as customer credit cards, once the information is stolen, the customer will no longer trust the company and will go to someone else who can protect their private information.

5.9 | Image Defamation

Nigerians' slogan, "good people great nation," will be tarnished by the high rate of cybercrime in the country, and the world will see things from a different angle. Other consequences include using computer and network resources and losing time and attention when people ignore unsolicited messages [27].

5.10 | External National Image

A country's external image serves as a mirror through which other nations see it when interacting. It is how different countries around the world view a nation. Image is one thing no nation, institution, government, group, or people can fool with. It is impossible to overlook impressions in everything one does. This is the case because one's perception shapes one's image, shaping the type of response or support one will receive from others. According to Soeze [28], a negative perception results in a negative image, which does not command “public support for any program of action.” Therefore, a negative image impacts a government or organization, particularly globally. Unfortunately, the country's reputation has also suffered due to a loss of integrity and trust in the world, which is a result of some Nigerians engaging in illegal activities that have made cyberspace a venue for criminal activity known as cybercrime [29].

5.11 | Retarded National Development

Cybercrime and insecurity are undoubtedly the greatest significant threat to national development efforts in Nigeria today. Cyber fraud hinders the nation's ICT industry's capacity growth, a key factor in the country's quick socioeconomic change. ICT development issues are crucial to any government's global development agenda. No country will be able to meet national development targets or the SDGs as we move farther into the uncharted territory of the digital revolution unless the hydra-headed monster of cybercrime is taken on head-on. Long-term national development efforts would suffer significantly if this burden is unresolved [30].

Theoretical explanations

This study explored social structure, Anomie theory, and Routine Activities Theory (RAT) to explain the causes of cybercrime among Nigerian youths.

6 | Social Structure and Anomie Theory

Durkheim's [31] theory of anomie and the functionalism theoretical tradition are the foundation for Merton's [32] social structure and anomie theory. The Greek word "anomos," which means "normlessness," is where Durkheim's [31] term "anomie" originates. An anomie society, according to Durkheim [31] in Siegel [16], is one in which the norms of behavior have been dismantled as a result of societal crises, fast social change, or the shift from a preindustrial to an industrial or urbanized social order [5], [11].

Durkheim [31] also tries to show how society's sociocultural structure influences people to commit crimes, arguing that deviant behavior and, implicitly, cybercrime tendencies are products of social structure. In keeping with the influence mentioned above, Merton [32] bases his theory of social structure and anomie on a modified form of the idea of anomie.

As people attempt to adjust to different means to achieve societal and cultural goals, the theory of the social structure of society states that an excessive emphasis on cultural goals at the expense of institutional means leads to an anomie tendency and, consequently, the proliferation of various crimes, including "cybercrime." However, Merton [32] contends in Siegel [16], starting from an American civilization, that cultural ideals like success, which is defined in terms of material possessions and wealth, are shared by all societies. Nonetheless, the same culture has established methods for success, including hard effort, skill, education, and so on.

According to Merton [32], institutional resources and cultural objectives are equally important in a balanced society [5]. Anomic societies place a high value on accomplishment despite having few or no resources to achieve it. Merton [32] asserts that people in later societies tend to disregard the game's rules and pursue achievement by whatever means necessary. According to Merton [32], people react to abandoned situations in the five adaption modes listed below, which explains crime in general and, implicitly, cybercrime:

I. The conformist: These people conform to the cultural goals of success and the institutional means. These people follow the legitimate means to succeed in life.

II. Innovation: These people reject normative means of achieving success; hence, their ways are blocked due to scarce legitimate means to success. Thus, they innovate by turning to deviance, such as cybercrime, and unemployed graduates who turn to armed robbery, which promises greater and quicker rewards.

III. Ritualism: In Merton's [32] sense, these people accept societal means but do not strive to achieve the cultural goals of success as society demands. Thus, a typical low-grade civil servant or school teacher is an example in this category.

IV. Retreatism: These people reject cultural goals and the institutional means of society, even when they internalize the duo. According to Merton [32], retreats resolve their conflict situations by giving to drugs, alcohol, and so on, and these categories of people are mostly outcasts, psychotics, vagrants, and so on [33].

V. Rebellion: These people reject both cultural goals of success and institutional means of success and seek to replace them with alternatives. Those that fall under this category are protesters, cyber terrorists, and revolutionaries.

According to social structure theory, most criminals are found within the innovation, retreatism, and rebellion adaption modes. Thus, by implication, cybercriminals in line with this theory can safely be located in the innovative adaption mode [5].

7 | Routine Activities Theory

One of the victimization hypotheses is the idea of routine activities. In other words, the theory focuses on the role of victims in the criminal process and the reasons for victimization. According to routine activities, the existence of motivated criminals, the lack of competent guardians, and the availability of appropriate targets can all contribute to crime rates. Therefore, the theory practically presupposes that three things must occur simultaneously and in the exact location for a crime to be committed.

According to Siegel [16], the theory demonstrates how a victim's actions can impact criminal opportunities and states that lowering target vulnerability and enhancing guardianship can reduce the chance of victimization. The volume and distribution of crime are closely linked to the interaction of three variables that represent "the routine activities of the typical American lifestyle," according to Cohen and Felon's [34] analysis in Siegel [16]. These variables include:

I. The availability of suitable targets, such as a home with readily available goods, a careless person, a house without a door, and a computer without a security PIN.

II. The lack of competent guardians, such as the police, homeowners, neighbors, friends, and family.

III. The existence of motivated offenders, such as a high percentage of young people without jobs, teens, men, drug users, provocative behavior, and so on.

All these elements raise the possibility of a crime, especially cybercrime. Additionally, according to the hypothesis, those who are the targets of criminal activity are more likely to become victims if they participate in dangerous behavior, are not well-protected, and are around a lot of motivated criminals, including adolescent males, young people without jobs, and drug addicts. The hypothesis is that if the aforementioned collection of people congregates in a given area, the place becomes a 'hot spot' for crime and violence. As a result, young men from Nigerian universities gather in schools to commit cybercrimes.

As with guardianship as a factor in crime, routine activity theory asserts that guardianship is more effective as deterrence if it comes from conventional peers who have been socialized to hold conventional attitudes. Siegel [16] also emphasizes that peer reaction and disapproval may be a form of moral guardianship that can deter even motivated offenders from engaging in law-violating behavior. Similarly, some young men who have not been adequately economically engaged tend to engage in criminal activities, particularly cybercrime, since it requires knowledge of computers and other technologies.

According to Schaefer [35], the theory also maintains that the presence of motivated offenders, the availability of suitable targets, and the lack of a capable guardian contribute to crimes and, implicitly, cybercrime. It also suggests that increasing guardianship and/or reducing target vulnerability can reduce the likelihood of victimization. The theory holds that crimes and, more importantly, cybercrimes are more likely to occur whenever offenders or cybercriminals come into contact with vulnerable targets, such as unsecured systems or networks, unpassworded systems, unencrypted email messages or chat forums, and so on.

In conclusion, the regular activities approach examines crimes from the perpetrator's perspective. According to the hypothesis, a crime will only be committed if a potential perpetrator believes the target is appropriate and there is no competent supervision personnel. It is the appraisal of a scenario that decides whether a crime will occur. Furthermore, the idea is limited by lifestyle and opportunity. Therefore, a person's living situation may impact victim risk. Similarly, residents of unsecured areas are vulnerable to determined criminals. A person's lifestyle influences the likelihood of crime since it determines their closeness to criminals, the amount of time they spend with them, and their desirability as a target of crime.

8 | Discussion

According to this study, cybercrime among Nigerian young is caused by several factors, including unemployment, the hunt for fast money syndrome, a corrupt culture, and a large percentage of criminally inclined adolescents. Regarding the implications of cybercrime, it has been found that it threatens national security, damages Nigeria's external national image, and lowers investor trust in the country's economy. Furthermore, Nigeria suffers from cybercrime because it hinders the country's sustainable development, jeopardizes national security, results in the loss of intellectual property, harms a company's reputation (if hacking took place), hinders technological advancement, damages the domestic economy, and lessens competitive advantages for development.

The findings of the factors that hinder cybercrime control in Nigeria are also noteworthy. According to the majority of respondents, the high rate of youth unemployment, the lack of database system technology, the lack of proactive measures to prevent cybercrime, the lack of tracking devices and mechanisms, the lack of cyber security to prevent hacking, the limitations in the investigation of cybercrime, and people with low incomes or lack of orientation to youths on the menace of cybercrime all work against the control of cybercrime in Nigeria.

9 | Conclusion

The threat of cybercrime has grown to be a significant habit among Nigerian youth. The issue has permeated every aspect of our culture and is dangerous to the nation's socioeconomic progress. Although cybercrime is a worldwide issue, the vulnerabilities and effects vary based on how well each nation implements countermeasures, such as cyber laws and cyber security technology. Nigeria is placed high amongst the cybercrime-afflicted nations since the country's reaction to mitigate cybercrime is still very poor owing to weak cybercrime legislation, limited technology, and lack of cyber security expertise.

Therefore, the lack of human capital in cyber-security is a significant risk element in meeting Nigeria's security demands to prevent cybercrime and cyber threats originating from cyber criminals. Based on these submissions, the study concludes that government and citizen efforts to reduce cybercrimes need to be redoubled because cyber security is essential to sustaining the provision of essential social services, preserving public confidence in information systems, and advancing socioeconomic development in Nigeria.

9.1 | Recommendations

Based on the findings above, recommendations were made to reduce the implication of cybercrime on the socioeconomic development and sustainability in Nigeria, such as:

I. The Nigerian government must aggressively use the media to raise public awareness of cybercrime, and the curriculum for elementary, secondary, and university education should include lessons on promoting personal cyberspace security.

II. People should follow basic personal safety guidelines, such as keeping personal belongings and financial information private, including credit card pins, bank account numbers, and email passwords, and using antivirus software to protect their computers from viruses.

III. The criminal justice system should ensure quick adjudication of cybercrime cases so that those found guilty can be punished according to the law. This would deter others from engaging in cybercrimes. Nigeria should apply new and current legislation (Acts) to lower the incidence of cybercrime. The government must pass comprehensive regulations to penalize criminals and successfully restrict the prevalence of cybercrime.

IV. The government needs to train special cybersecurity experts while aiding the existing law enforcement, intelligence, and security agencies in understanding the nature of technology and the individuals involved in cybercrime.

V. Parents should use content filtering software on computers to protect children from cybercriminal activities. This will reduce the incidence of cybercriminality among Nigerian teenagers and youth.

Author Contributions

SIA: Conceptualization, writing - original draft, resources; OSF: Writing, analysis; MA: Writing, visualization.

The authors read and approved the final manuscript.

Institutional Review Board Statement

Not applicable.

Data Availability

The study has no associated data.

Funding

This research received no external funding.

Acknowledgment

The author appreciates the editor and reviewers for adding valuable input to the manuscript.

Clinical Trial Number

Not applicable

Informed Consent Statement

Not applicable.

Availability of Data and Materials

Not applicable

Conflicts of Interest

The author declares that there is no competing interest.

References

[1] Adeniran, A. O. (2016). Impacts of the fourth industrial revolution on transportation in the developing nations. *International educational scientific research journal*, *2*(11), 56–60. https://core.ac.uk/download/pdf/234690193.pdf

[2] Adeniran, A. O., Onuajah, S. I., Adeniran, A. A., & Ogunmola, M. A. (2024). Implementing cloud-centric IoT transformations: Merits and demerits. *Systemic analytics*, *2*(2), 174–187. https://B2n.ir/fg6619

[3] Adeniran, A. O., Jadah, H. M., & Mohammed, N. H. (2020). Impact of information technology on strategic management in the banking sector of Iraq. *Insights into regional development*, *2*(2), 592–601. https://dx.doi.org/10.9770/IRD.2020.2.2(7)

[4] Paranjape, N. V. (2010). *Criminology and penology*. Central Law Publications. https://www.clplawbooks.com/book_detail/234

[5] Idowu, O. A., & Madaki, M. (2021). Cybercrimes and challenges of cyber-security in Nigeria. *International journal of sociology and development*, *3*(1). https://www.academia.edu/download/68256782/2021_Cybercrime_and_the_Challenges_of_Cyber_Security_in_Nigeria.pdf

[6] Guterres, A. (2020). *The sustainable development goals report 2020*. https://B2n.ir/ds6691

[7] Adeniran, A. O. (2019). Anti-corruption policy strategies for Nigeria towards national development: Evidence from least corrupt countries. *American international journal of social science research, 4*(2), 1–8. https://B2n.ir/qm6050

[8] Adesina, O. S. (2017). Cybercrime and poverty in Nigeria. *Canadian social science*, *13*(4), 19–29. https://dx.doi.org/10.3968/9394

[9] Ayofe, A. N., & Oluwaseyifunmitan, O. (2009). Towards ameliorating cybercrime and cybersecurity. *International journal of computer science and information security*, *3*(1), 1–11. https://arxiv.org/pdf/0908.0099

[10] Uroko, F. C. (2020). Jethro's mentoring of moses (exodus 18) and its relevance to the Nigerian clergy. *E-journal of religious and theological studies*, *6*(2), 135–144. https://B2n.ir/by8345

[11] Dambazau, A. R. B. (1999). *Criminology and criminal justice*. Nigerian Defence Academy Press. https://B2n.ir/ff6400

[12] Ibrahim, U. (2019). The impact of cybercrime on the Nigerian economy and banking system. *NDIC quarterly*, *34*(12), 1–20. https://nigeriareposit.nln.gov.ng/items/7d8a3a8c-17c8-4114-83c5-644f98672c55

[13] 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. https://B2n.ir/gr4660

[14] James, A. (1993). *Introduction to information system*. Amazon. https://B2n.ir/yu4784

[15] Shinder, D. L., & Tittel, E. (2002). *Scene of the cybercrime: Computer forensics handbook*. Rockland, MA: Syngress Publishing. https://B2n.ir/wt3870

[16] Siegel, L. J. (2004). *Criminology: Theories, patterns and typologies*. USA: Wadsworth, a Division of Thompson Learning Inc. https://B2n.ir/zn9460

[17] Kudi Dukk, M. (2019). The nature, causes and consequences of cyber crime in tertiary institutions in in tertiary institutions in gombe, gombe gombe, gombestate, Nigeria .*International journal of educational research and management technology, 4*(1).100-115. https://B2n.ir/de5870

[18] Golubev, V. (2005). *International cooperation in fighting cybercrime*. https://B2n.ir/wp4583

[19] Oyewole, A. S., & & Obeta, A. (2002). *An introduction to cybercrime.* http://www.crimeresearch.org/artilces/cybercrime.

[20] Ehimen, O. R., & Bola, A. (2010). Cybercrime in Nigeria. *Business intelligence journal*, *3*(1), 93–98. https://B2n.ir/qr2282

[21] Ribadu, N. (2007). *Cybercrime and commercial fraud: A Nigerian perspective*. UNCITRAL. https://B2n.ir/mn4377

[22] Olugbodi, K. (2010). *Fighting cybercrime in Nigeria.* https://B2n.ir/wb5524

[23] Adeniran, A. O. (2018). Assessment of Federal governments' effort on looted assets recovery in Nigeria as a means of fighting corruption and terrorism. *Discovery*, *54*(276), 453–462. https://B2n.ir/qk2562

[24] Awe, J. (2009). *Fighting cybercrime in Nigeria*. http://www.jidaw.com/itsolutions/security3.html.

[25] Siebel, T. M., & House, P. (1999). *Cyber rules: Strategies for excelling at e-business*. Doubleday. https://B2n.ir/hj4272

[26] Broad, J. (2013). *Risk management framework: A lab-based approach to securing information systems*. Newnes. https://B2n.ir/my4342

[27] Onodugo, I. C., & Itodo, S. M. (2016). Cyber crime and Nigerian business environment. *National journal of advanced research*, *2*(2), 28–38. https://B2n.ir/uf6952

[28] Soeze, C. I. (2014). *Laundering Nigeria's international image*. https://B2n.ir/bb3190

[29] Abdul-Rasheed, S. L., Lateef, I., Yinusa, M. A., & Abdullateef, R. (2016). Cybercrime and Nigeria's external image: A critical assessment. *Africology: the journal of pan african studies*, *9*(6), 119–132. https://B2n.ir/qk4410

[30] Ugwu, U. D., & & Bassey, O. (2018). Cybercrime as an emergent security issue in Nigeria: Implications for national development. *International journal of scientific and engineering research*, *9*(6), 990 – 1000. https://B2n.ir/wr9989

[31] Durkheim's, E. (1933). *Theory, legacy & structural functionalism*. Social Science Courses. https://B2n.ir/eb4315

[32] Merton, R. K. (1968). *Social theory and social structure*. Simon and Schuster. https://B2n.ir/eg6833

[33] Olorunfemi, S. O., Adeniran, A. O., & Amoako-Sakyi, R. O. (2024). Conflict among the national union of road transport workers in Akure, Nigeria: Causes, consequences and management strategies. *Discover global society*, *2*(1), 41. https://doi.org/10.1007/s44282-024-00069-1

[34] Cohen, L. E., & Felson, M. (2010). Social change and crime rate trends: A routine activity approach (1979). In *Classics in environmental criminology* (pp. 203–232). Routledge. http://dx.doi.org/10.2307/2094589

[35] Schaefer, R. T. (2005). *Sociology*. McGraw Hill Company. https://B2n.ir/pq8773