THE DOUBLE-EDGED SWORD OF DIGITAL CONNECTIVITY: ADVANCING SOCIETY AND EMPOWERING CYBERCRIMINALS

Akinola Festus ODESANMI
Department of Sociology, Landmark University, Omu-Aran, Nigeria
Email: odesanmi.akinola@lmu.edu.ng

***Oladayo Aveez IBITOYE**
Department of Educational Foundations and Counselling
Achievers University, Owo, Ondo State. Nigeria.
Emails: ibitoye.oa@achievers.edu.ng

Oluwakemi IWELUMOR
Department of Sociology, Landmark University, Omu-Aran, Nigeria
Email: babatunde.oluwakemi@lmu.edu.ng

Henry OBUENE
Department of Sociology, Landmark University, Omu-Aran, Nigeria
obuene.henry@lmu.edu.ng

Oluwatosin Tobi AROWOLO
Department of General Studies, Federal Cooperative College, Eleyele, Ibadan, Nigeria
Email: 123t.morenike@gmail.com

Ilesanmi Daniel OLUSEGUN
Department of Criminology and Security Studies
Thomas Adewumi University, Oko-Irese, Nigeria
Email: olusegun.daniel@tau.edu.ng

David DUROJAIYE
Department of Sociology, Landmark University, Omu-Aran, Nigeria
Email: durojaiye.david@lmu.edu.ng
*Corresponding Author: ibitoye.oa@achievers.edu.ng

Abstract

Digital connectivity has significantly reshaped modern society, revolutionising how individuals communicate, access services, and conduct businesses. This transformation has promoted economic growth, improved productivity, and enhanced social inclusion. However, alongside these benefits, there has been an upsurge in cybercrime. This has led to palpable fear among individuals, organisations, and governments. This article, therefore, reviewed the double-edged sword of digital connectivity, its origin, impacts, and factors contributing to this crime. The study used secondary data including websites, magazines, newspapers, books, articles and journals as essential foundation for this study. To bridge the gaps from previous researchers, Social learning theory (SLT) was used to explain how individuals, their environment, and behaviours interact with others to engage in cybercriminal activities through observation, imitation, and reinforcement. It also presents a case study to examine the underlying factors contributing to cybercrime in Nigeria, offering insights into the socio-technical dynamics that enable its growth. Nevertheless, as dependence on digital technologies intensifies, the associated vulnerabilities to cyber threats have become increasingly complex and pervasive. Addressing this challenge necessitates a collaborative, multi-stakeholder approach encompassing governmental bodies, the private sector, academia, and civil society to maintain technological advancement and public trust.

Keywords: Digitisation, Cybercrime, Impacts, Law Enforcement, Nigeria

Introduction

In today's digital age, technological advancements have transformed how individuals and organisations communicate, conduct business, and interact. This is made possible by widespread use of the internet and mobile devices. However, these have driven the digitisation of society, and at the same time, the digitisation of crime, resulting to new types of offences, such as hacking into systems and databases, disrupting websites, and entire networks. Consequently, traditional crimes such as fraud, forgery, and data theft, have evolved with information and communication technology (ICT) playing a growing role in facilitating activities such activities through email and social media (Auwal, 2023; Holt, 2019). These trends have led to increasingly complex and sophisticated threats affecting individuals, private and public sectors, leading to significant annual financial losses (Holt, 2019). This (ICT) affects productivity, investment, and innovation. It also results in reputational harm, and socially contributes to a growing sense of insecurity in digital environments (Marcelino, 2022).

This nefarious activity is known as cybercrime (Marcelino, 2022; Awhefeada & Bernice, 2020). Cybercrime encompasses any criminal activity involving computers, smartphones, networks, and other digital devices to commit illegal acts (Marcelino, 2022). These crimes include hacking, phishing, identity theft, online fraud, cyberstalking, data breaches, ransomware attacks, and the distribution of malicious software (Awhefeada & Bernice, 2020). Perpetrators range from individuals and organised groups to state-sponsored actors, often targeting individuals, businesses, or governments to steal data, disrupt operations, or exploit weaknesses for financial or strategic advantage (Verizon, 2023).

These acts poses a threat to global security, privacy, and economic stability (Sutardi & Ferdiles, 2023; Marcelino, 2022). The issue of cybercrime cannot be completed without mentioning cyberspace. Cyberspace is a global network of interconnected electronic, wireless, and optical communication technologies that facilitate the exchange of data and communication on a worldwide scale (Adewopo et al. 2024). It comprises of millions of interconnected networks from local to international across private, public, academic, business, and government sectors. It is through cyberspace that users access information, share content, send messages, and utilise various online services via web browsers, apps, and digital platforms (Adewopo et al. 2024; Makeri, 2017). Similarly, the role of the internet cannot be overemphasised. The Internet is defined as a vast system of electronically linked devices such as smartphones, vehicles, televisions, radios, and smartwatches. Internet service providers (ISPS) in Nigeria, such as MTN and Globacom, enable users to connect to the network. This gives them access to social media platforms, video conferencing, digital content, and e-commerce services (Alabi et al., 2023; Makeri, 2017). While the internet is the infrastructure that enables connectivity, cyberspace represents the virtual environment created through that connectivity, including all forms of online interactions, digital content, and virtual platforms where data is generated, exchanged, and stored. Though not a physical space, cyberspace is the conceptual realm where activities such as social networking, e-commerce, gaming, and even cybercrime take place. Essentially, anything conducted through the internet happens within the domain of cyberspace. Thus, access to cyberspace is dependent on the internet, and all internet-based activities are carried out within it (Adewopo et al. 2024; Alabi et al. 2023).

In tackling cybercrime, the law enforcement agencies traditionally responsible for maintaining public safety and enforcing the law now face a distinct challenge of addressing crimes that transcend physical borders, often concealed by digital anonymity. Cybercrime requires advanced technological tools and specialised expertise, and at the same time comprises of robust international collaboration to operate across multiple jurisdictions. Therefore, as the frequency and complexity of these crimes grow, the role of law enforcement agencies becomes ever more vital in combating these dangers and ensuring a safe digital space (Sutardi & Ferdiles, 2023).

Theoretical Framework

This study uses Akers's Social learning theory (SLT). SLT explains how individuals, their environment, and behaviours interact with others. This interaction takes place through observation, imitation, and reinforcement. In the context of cybercrime, SLT suggests that individuals engage in cybercriminal activities by learning from their peers, online communities, or media influences (Akers, 2017).

The first component of this theory is differential reinforcement. This theory proposes that exposure to a digital platform environment where illegal techniques, criminal justifications, and mentorship from experienced hackers are located increases the likelihood that individuals will engage in cybercrime (Odesanmi, et al. 2023; Akers, 2017). For instance, when individuals join forums that share tips on hacking or cyber fraud, they gradually absorb the necessary skills and learning the language of criminality. Similarly, individuals within these groups often reinforce each other's behaviour by fostering a sense of community and belonging. This creates a social norm where cybercrime is seen as not only acceptable but potentially rewarding (Dearden, & Parti, 2021).

Imitation, as the second component, posits that individuals are often inspired to replicate (model) the actions of successful or infamous cybercriminals (Akers, (Ed.). 2017). Examples are the publicisation of high-profile attacks, such as ransomware incidents or data breaches. Such publicisation not only increases the visibility of cybercrime but also motivates others to try to replicate these crimes for financial gain or reputational recognition (Odesanmi, et al. 2023; Holt, 2019).

The third component is definitions, and encompasses personal beliefs, justifications, and rationalisations that individuals hold. These play a significant role in shaping whether or not someone engages in cybercrime. According to this theory, those who rationalise cybercriminal actions as acceptable, harmless, or justified are more likely to engage in illegal activities. Common justifications include viewing hacking as digital activism, justifying piracy as fair redistribution, or rationalising theft as a form of retribution against perceived economic inequalities. These definitions minimise the moral concerns individuals might otherwise have and encourage the continuation of cybercrime (Miller, & Morris, 2016). Akers' Social learning theory highlights how cybercrime is not just a result of individual choice but also a learned behaviour influenced by social interactions, online communities, and perceived rewards.

Literature Review

The Origins of Cybercrime

Cybercrime has its roots in the early days of computing and the internet, evolving alongside technological advancements. According to historical evidence, from the 1960s to the 1980s, hacking transitioned from simple curiosity-driven experiments to more complex methods (Babanina, Tkachenko, Matiushenko & Krutevych, 2021). This prompted the introduction of laws to address unauthorised access to computer systems. Initially, the term "hacker" referred to skilled programmers and engineers who aimed to push the boundaries of early computer systems. For example, In the Tech Model Railroad Club (TMRC), students began manipulating mainframe computers to enhance their performance. Therefore, these early hackers were not criminals, but rather computer enthusiasts trying to understand and improve existing technologies (Babanina et al. 2021). However, in the 1970s, as computer networks were expanding, a new phenomenon emerged known as phone phreaking. This practice involved manipulating telephone systems to make free long-distance calls, leading to unauthorised access (Ibrahim, et al. 2024). This became a popular underground activity, with groups of individuals sharing knowledge on how to exploit the telephone network (Schjolberg, 2020).

The 1980s marked a significant shift in hacking, as it moved from curiosity-driven exploration to activities with serious security implications. For example, in 1982, a 15-year-old Rich Skrenta created one of the first known computer viruses, Elk Cloner, which spread via infected floppy disks on Apple II computers. Although the virus displayed a playful message, it highlighted the potential dangers of self-replicating code (Ibrahim, et al. 2024). With the rise of hacking incidents, governments began to acknowledge the need for legal frameworks to address unauthorised computer access. This led the United States to pass the Computer Fraud and Abuse Act (CFAA) in 1986, criminalising unauthorised access to computer systems and laying the foundation for modern cybersecurity laws (Babanina, Tkachenko, Matiushenko & Krutevych, 2021).

The commercialisation of the World Wide Web in the early 1990s expanded internet access, creating new opportunities for cyber threats. Without mincing words, as businesses and financial institutions began offering online services, they were at the same time becoming prime targets for cybercriminals from an intellectual pursuit to a tool for financial gain, espionage, and disruption (Ibrahim, et al. 2024). Similarly, in 1994, Kevin Mitnick breached the computer networks of major corporations, stealing proprietary software and sensitive data. This was done by employing social engineering tactics to manipulate employees into granting him access to critical systems. His actions exposed significant vulnerabilities in corporate cybersecurity, leading to one of the FBI's most high-profile investigations, culminating in his arrest in 1995 (Schjolberg, 2020). In the same vein, in 1998, a hacker known as "Mafiaboy" executed one of the first documented Denial of Service (Dos) attacks on several university networks, disrupting their online services. These attacks revealed how cybercriminals could create widespread disruptions using relatively simple techniques (Ibrahim, et al. 2024). The 1990s also saw the rise of malware, including keyloggers, which secretly record keystrokes to capture sensitive information such as usernames, passwords, and credit card numbers, and Trojans, that masqueraded as legitimate software while performing malicious actions in the background, giving hackers remote control over infected systems(Babanina, Tkachenko, Matiushenko & Krutevych, 2021; Schjolberg, 2020).

The era of the 2000s marked a dramatic increase in financially motivated cybercrime and the rise of nation-state cyberattacks. The ILOVEYOU worm demonstrated the destructive potential of email-based malware, while the growth of cybercriminal markets fueled identity theft and financial fraud. For example, the 2007 cyberattack on Estonia introduced a new era of cyber warfare, and the Conficker worm highlighted the escalating challenge of large-scale malware infections. These incidents helped shape modern cybersecurity policies and defences, and at the same time influenced how nations and organisations address digital threats (Schjolberg, 2020). Additionally, between 2005 and 2010, cybercrime evolved into a more organised and commercialised underground economy, where hackers sold stolen credit card information, hacking tools, and personal data on the dark web. By this time, criminal groups developed sophisticated techniques to evade detection and maximise profits (Ibrahim, et al. 2024). Between 2005 and 2010, cybercrime has evolved into a highly advanced global threat, fueled by Advanced Persistent Threats (APTs), ransomware, AI-driven attacks, and state-sponsored cyber warfare. Cybercriminals have now being increasingly utilising automation, deepfake technology, and cryptocurrency to carry out financially and politically motivated cybercrimes (Borghard & Lonergan, 2021).

Types of Cybercrime

Cybercrime is broadly classified based on the nature of the offence and the intent behind it. The most common forms include:

Hacking: This refers to unauthorised access, manipulation of computer systems, networks, or data. It also involves exploiting software vulnerabilities, using phishing techniques to steal login credentials, or launching brute-force attacks to crack passwords. It should be noted here that while some hackers seek financial gain, others engage in hacking for espionage, activism, or personal retaliation (Ibrahim, et al. 2024).

Phishing: Phishing is a deceptive tactic in which cybercriminals impersonate trusted entities to trick individuals into divulging sensitive information such as passwords, credit card details, or personal data. Attackers often pose as banks, government agencies, or reputable companies through fraudulent emails, fake websites, or misleading messages (Marcelino, 2022).

Ransomware and Malware Attacks: These involve the deployment of malicious software to infect systems, lock users out, and demand ransom payments in exchange for decryption, usually in cryptocurrency to remain anonymous. They target individuals, businesses, and government institutions. Trojan horses are often used to steal sensitive data, while spyware monitors and tracks user activity (American Psychological Association. 2023).

Cyberbullying: Cyberbullying, also known as cyberstalking or online harassment, involves using digital platforms such as social media, messaging apps, and online forums to intimidate, stalk, or harm individuals. This includes spreading false rumours, sharing private or embarrassing content, sending threats, and engaging in non-consensual sharing of personal images (Ibrahim, et al. 2024; Marcelino, 2022).

Financial and Banking Fraud: This encompasses illegal activities involving deception, manipulation, and misrepresentation to unlawfully obtain money, assets, or financial information through online banking systems and financial platforms. These crimes are committed by individuals, businesses, or even financial institutions (Ibrahim, et al. 2024).

Online Child Exploitation and Abuse: This is the use of the internet to exploit minors for sexual, financial, or criminal purposes. It involves manipulation, coercion, and deception through social media, gaming platforms, and dark web networks. Examples include the distribution of child pornography, online grooming, and human trafficking facilitated through encrypted online platforms (Ibrahim, et al. 2024).

Intellectual Property Theft and Piracy (IP): IP refers to creations of the mind, such as literary works, inventions, and trademarks, which are protected by copyright and patent laws. IP theft or piracy involves unauthorised use, reproduction, or distribution of protected works without permission. Common forms include software piracy, illegal streaming of music and movies, and the theft of trade secrets (Marcelino, 2022).

Fake News and Misinformation: It is a deliberate spread of false or misleading information disguised as legitimate news to manipulate public opinion. It may be entirely fabricated or a blend of truth and falsehoods, often circulated through social media, websites, and traditional media outlets. Misinformation, on the other hand, involves the unintentional spread of inaccurate information due to misunderstandings, misinterpretations, or reliance on unverified sources, including rumours, outdated data, and misattributed statements (Ibrahim, et al. 2024; American Psychological Association, 2023).

Identity Theft and Fraud: Identity theft and fraud involve the unauthorised acquisition of personal information to impersonate someone for financial gain or other illegal activities. This serious crime results in financial losses, reputational harm, and legal consequences for the victim. Common examples include credit card fraud, social security number theft, and fraudulent loan applications (Urhibo, 2021).

Cyberterrorism: This is the use of digital technology and cyberattacks by individuals or groups to disrupt critical systems, instil fear, damage infrastructure, or support terrorist activities. These attacks are often motivated by ideological or political objectives and can be launched from anywhere, making detection and prevention challenging. This includes breaches of government databases, the spread of propaganda or misinformation, and cyberattacks on essential infrastructure such as power grids, hospitals, and transportation systems (Ibrahim, et al. 2024).

An Overview of Cybercrime in Nigeria

Nigeria, with one of the highest internet usage rates in Africa, has seen a surge in cybercriminal activities due to increased internet penetration and inadequate cybersecurity measures. This has become a significant challenge, affecting individuals, businesses, and the government, with prevalent crimes. In response to incessant internet penetration, the Cybercrime Act of 2015 was introduced by the Nigerian government to serve as the first cybercrime legal and regulatory structure. Through this act, the law enforcement agencies were given the mandate to control people's actions in cyberspace as well as to prohibit and deter cybercrime (Urhibo, 2021). The act also establishes a unified, effective, and comprehensive legal, administrative, and regulatory framework to prevent, investigate, identify, prosecute, and penalise cybercrime and related offences (Makeri, 2017; Ajayi, Amorighoye & Osayi, 2025). According to Ajayi, Amorighoye & Osayi, (2025), Urhibo, (2021), Awhefeada & Bernice (2020), and Makeri, (2017), the objectives outlined for each section are: Section 1 of the Act aligns closely with those stated in the Act's explanatory memorandum. Furthermore, Section 2 affirms that "the provisions of this Act shall apply throughout the Federal Republic of Nigeria.

The Act is structured into 59 sections, divided across 8 parts and 2 schedules.
Part I (Sections 1–2) covers the objectives and scope of the application.
Part II (Sections 3–4) focuses on the protection of critical national information infrastructure.
Part III (Sections 5–36) details offences and corresponding penalties. This includes attacks on critical national infrastructure, unauthorised access to computer systems, regulation of cybercafés, system and network interference, interception of emails and financial transfers, tampering with infrastructure, misrouting of electronic messages, computer-related forgery and fraud, theft of electronic devices and data; cyber terrorism, fraudulent issuance of electronic instructions, identity theft and impersonation, child pornography, cyberstalking and cybersquatting, racist and xenophobic content, importation or creation of electronic crime tools, ATM/POS manipulation and, unauthorized card use.
Part IV (Sections 37–40) outlines the responsibilities of financial institutions and service providers.
Part V (Sections 41–44) addresses administrative roles and enforcement mechanisms.
Part VI (Sections 45–49) focuses on procedures for arrest, search, seizure, and prosecution.
Part VII (Sections 50–56) deals with jurisdictional matters and international cooperation.
Part VIII (Sections 57–59) includes miscellaneous provisions, including regulations, definitions, and the citation of the Act.
The First Schedule specifies the members of the Cybercrime Advisory Council, while the Second Schedule lists the categories of businesses required to contribute to the National Cybersecurity Fund, as stipulated in Section 44(2) (a) of the Act.

Factors Contributing To the Rise of Cybercrime in Nigeria

There are several factors contributing to the rise of cybercrime in Nigeria. Some of the factors are discussed hereunder.

i. The persistent issue of youth unemployment in Nigeria has significantly contributed to the growth of cybercrime. Many young individuals with technological skills, but limited job opportunities, turn to illicit online activities as a means to earn a living or quickly acquire financial gains (Ajayi, Amorighoye & Osayi, 2025; Urhibo, 2021). Similarly, the lack of robust cybersecurity systems within both the public and private sectors leaves critical networks and data vulnerable to breaches. This inadequate infrastructure creates an environment ripe for exploitation by cybercriminals (Auwal, 2023).

ii. Law enforcement's ability to effectively combat cybercrime is hindered by outdated laws, a lack of technical expertise, and bureaucratic inefficiencies within the judicial system. This legal gap allows cybercriminals to operate with relative impunity (Urhibo, 2021). In the same vein, the rapid growth of Internet access and smartphone usage in Nigeria, while beneficial for communication and commerce, has inadvertently expanded the opportunities for cybercriminals. The increased number of access points creates more opportunities for unsuspecting victims to be targeted (Auwal, 2023).

iii. A widespread lack of digital literacy and cybersecurity education leaves individuals and organisations vulnerable to phishing, malware, and other cyberattacks. This ignorance makes it easier for cybercriminals to deceive and exploit users (Awhefeada & Bernice, 2020; Alabi, Bamidele & Oladimeji, 2023). Furthermore, significant disparities in wealth distribution and access to economic opportunities drive individuals, particularly those from disadvantaged backgrounds, to resort to cybercrime as a coping mechanism or form of protest against systemic inequalities (Alabi, Bamidele & Oladimeji, 2023; American Psychological Association. 2023).

iv. Widespread corruption within institutions, including law enforcement agencies, hampers the effective enforcement of cybersecurity policies. This corruption allows offenders to avoid detection, investigation, and prosecution, thereby perpetuating the cycle of cybercrime (Ajayi, Amorighoye & Osayi, 2025).

v. To crown it all, Nigeria's integration into the global digital economy, while facilitating international communication and trade, has also exposed its digital ecosystem to more sophisticated and transnational cyber threats. Cybercriminals exploit global tools, platforms, and networks to carry out complex operations that extend beyond national borders (Awhefeada & Bernice, 2020).

General Impacts of Cybercrime

Cybercrime has far-reaching consequences for individuals, businesses, and governments, leading to financial, psychological, legal, and security challenges.

Cybercrime results in substantial losses that arise from various cyber threats to gain unauthorised access to financial accounts (Verizon, 2023). Major contributor to financial losses is ransomware attacks, in which cybercriminals encrypt an organisation’s data and demand ransom for decryption. Beyond the ransom payments, businesses often suffer reputational damage, regulatory fines, and costly recovery efforts, including IT infrastructure repairs and system rebuilding (Holt, 2019). In the same vein, industries that experience data breaches may face legal penalties for failing to protect sensitive customer information, further increasing their financial burden (IBM, 2023). Economic impact of cybercrime is staggering, with global losses reaching trillions of dollars annually, making it more profitable than the global drug trade (Forrester. 2023).

Data breaches pose a significant threat to individuals, businesses, and governments, as cybercriminals exploit sensitive information for financial gain or strategic advantage. Similarly, government agencies are also vulnerable to cyber espionage, where state-sponsored hackers infiltrate secure networks to access classified information, posing serious risks to national security (Verizon, 2023). Effects are that a data breach damages an organisation’s reputation, eroding public trust. Consumers and business partners may lose confidence in a company’s ability to protect their data, leading to lost business opportunities and declining stock values (IBM, 2023). Additionally, stolen personal information are frequently used for identity theft. Victims may suffer from unauthorised transactions, fraudulent loans, and long-term financial hardships (Holt, 2019).

Reputational damage to businesses and individuals leads to financial losses, legal repercussions, and social stigma. This is evidenced by cybercriminals often using stolen personal data for extortion, threatening to release private photos, financial details, or sensitive communications (Holt, 2019). While individuals can face defamation, companies that experience cyber incidents often struggle to retain customers, and publicly traded organisations may see a sharp drop in stock prices (Forrester. 2023). Furthermore, organisations hit by cyberattacks may face lawsuits and regulatory fines. Rebuilding trust after a cyber-incident may take years and requires significant investments in public relations, cybersecurity enhancements, and customer compensation programs (IBM, 2023).

Cybercrime extends beyond financial and reputational harm, often causing severe psychological and emotional distress for victims. Cyberbullying, including harassment, online shaming, and doxxing, leads to significant emotional turmoil (Holt, 2019). Victims of identity theft frequently experience feelings of powerlessness, insecurity, and vulnerability. Many also suffer from heightened anxiety, paranoia, and sleep disturbances upon discovering that their personal information has been misused (American Psychological Association. 2023). In the same vein, entrepreneurs dealing with financial losses, legal battles, and reputational damage may experience anxiety, depression, and burnout (Holt, 2019). Additionally, the stress of informing customers and stakeholders about a data breach further exacerbates their emotional burden, and victims of cybercrime often develop post-traumatic stress disorder (PTSD), depression, and anxiety, which can interfere with their ability to work or carry out daily activities (Europol. 2022).

The disruption of business and critical services results in downtime, financial losses, and even risks to public safety? For example, ransomware, Denial of Service (Dos) attacks, and cyberattacks on critical infrastructure such as power grids cause blackouts and have far-reaching consequences, impacting economic stability and essential services (American Psychological Association. 2023). Businesses lose millions in revenue when operations are halted due to cyberattacks. On a larger scale, cyber incidents destabilise national economies. Attacks on healthcare, energy, and government institutions pose threats beyond financial damage; disruptions in emergency services, hospitals, or critical infrastructure can lead to life-threatening consequences and national security risks (Europol. 2022).

Cyberattacks have become a critical national security issue, with governments and military institutions frequently targeted through cyber espionage, cyberterrorism, and cyberwarfare. Attacks on critical infrastructure such as power grids, water treatment facilities, and communication networks pose significant risks to national stability and public safety (Holt, 2019). Cyber espionage not only endangers national security but also provides adversarial nations with strategic advantages. For example, election interference through cyberattacks, misinformation campaigns, and the hacking of voting systems undermines democratic institutions and erodes public trust (Senate Intelligence Committee, 2020; Europol, 2022).

As cyber threats grow in frequency and sophistication, businesses and governments are investing heavily in cybersecurity to mitigate risks. The financial burden includes hiring specialised cybersecurity professionals, deploying advanced security measures, and conducting continuous security training. However, despite these investments, cybercriminals continuously evolve their tactics, requiring organisations to remain vigilant and proactive

(Gartner, 2022). Therefore, as governments are enforcing stricter data protection and laws, organisations are allocating further resources to ensure regulatory compliance. All these further drive up cybersecurity expenditures (Forrester, 2023).

The Role of Law Enforcement in Combatting Cybercrime

Investigation: Law enforcement agencies play a vital role in detecting, analysing, and preventing cybercrime by collecting digital evidence, tracing cyberattacks, and identifying perpetrators. They utilise advanced forensic tools to monitor online activities, recover deleted files, and decrypt encrypted communications. Investigations often involve tracking activities on the dark web, analysing financial transactions, and collaborating with cybersecurity experts to uncover sophisticated cyber threats. This proactive approach enhances threat detection and enables effective responses to cybercriminal activities (Sutardi & Ferdiles, (2023; Gartner, 2022).

Collaboration: Given the global nature of cybercrime, law enforcement agencies work closely with both domestic and international organisations to tackle cyber threats that extend beyond national borders. Agencies such as Interpol, Europol, and national cybercrime units collaborate with cybersecurity firms, intelligence agencies, and private sector entities to share intelligence, coordinate investigations, extradite cybercriminals, and harmonise legal frameworks. This international cooperation is essential for maintaining global cybersecurity and protecting businesses, governments, and individuals from cyber threats (Aldoghmi, 2024; Urhibo, 2021).

Prevention: In addition to investigations and enforcement, law enforcement agencies focus on preventive measures to reduce cybercrime incidents. Drawing from their expertise, they provide guidance to governments on cybersecurity regulations and policies to strengthen national security, economic stability, and public safety. They also conduct public awareness campaigns, educational initiatives, and training programs to educate individuals and businesses on cybersecurity threats and best practices (Aldoghmi, 2024). Furthermore, they develop national strategies for responding to cyberattacks, including crisis management, forensic investigations, and recovery efforts. They also promote secure online behaviours, advocate for strong passwords, and raise awareness about phishing scams. Through these efforts, law enforcement helps individuals and organisations protect themselves against cyber threats (Leenen, Van Vuuren & Van Vuuren, 2020).

According to Senate Intelligence Committee (2020), several major agencies play a crucial role in the fight against cybercrime worldwide. The Federal Bureau of Investigation (FBI) is responsible for handling major cybercrime cases in the United States, including cyber terrorism and large-scale financial fraud. The European Union Agency for Law Enforcement Cooperation (Europol) supports member states in combating cyber threats across Europe (Europol, 2022). Additionally, Interpol facilitates international police cooperation, focusing on transnational cybercrime and coordinating global law enforcement efforts (Forrester, 2023).

Challenges Faced By Law Enforcement in Combating Cybercrime

Without mincing words, law enforcement is faced with numerous challenges in discharging its duties. Some of the challenges are:

i. Rapid Technological Advancements: Cybercriminals continuously evolve their tactics, leveraging on emerging technologies to develop more sophisticated attack methods. Threats such as artificial intelligence-driven cyberattacks, quantum computing risks, and deepfake technology pose significant challenges for law enforcement agencies (Holt, 2019). The fast-paced evolution of technology requires agencies to constantly update their skills, tools, and investigative techniques to stay ahead of cybercriminals (Auwal, 2023).

ii. Jurisdictional Challenges: Cybercrime often crosses national borders, creating complex legal and diplomatic challenges, as criminals may operate from one country while targeting victims in another. This complicates the enforcement of laws and prosecution efforts. Similarly, the use of anonymisation techniques and geographically dispersed servers further hinders investigations, because variation in legal frameworks, extradition policies, and international cooperation levels can slow down the pursuit of cybercriminals. Although agencies like Interpol and Europol facilitate cross-border collaboration, jurisdictional conflicts remain a significant barrier to effective cybercrime enforcement (Sousa-Silva, 2024).

iii. Resource Limitations: Many law enforcement agencies, particularly in developing countries, face significant challenges due to limited resources. These include insufficient funding, inadequate training, and outdated technology. These hinder the effective use of advanced forensic tools necessary to combat cybercrime. Additionally, the private sector often possesses more sophisticated cybersecurity capabilities, creating a disparity between law enforcement and cybercriminals who exploit these vulnerabilities (Adewopo et al. 2024; Leenen, Van Vuuren & Van Vuuren, 2020).

iv. Digital Evidence: Collecting and preserving digital evidence presents challenges due to its volatile nature and the necessity of maintaining its integrity. Law enforcement agencies are therefore required to adhere to protocols by ensuring that digital evidence remains admissible in court. However, the absence of standardised procedures and regulations for handling digital evidence can undermine its credibility and admissibility during legal proceedings (Marcelino, 2022).

v. *Anonymity and Encryption:* Cybercriminals frequently utilise anonymity tools and encryption to hide their identities and activities, making it difficult for law enforcement to identify and apprehend offenders. The use of decentralised applications (DApps) adds another layer of complexity to investigations, as these platforms lack centralised servers, making it difficult to trace connections between accounts and real-world identities (Holt, 2019).

There have been notable investigations where Nigerian law enforcement, in collaboration with international agencies, has successfully dismantled cybercrime rings. These instances provide valuable insights into the potential for effective cross-border cooperation. However, despite some successes, many operations continue to elude authorities due to the anonymity of online activities, sophisticated encryption techniques, and the rapid evolution of digital tools (Urhibo, 2021).

Conclusion and Suggestions

This study reviewed literature on the double-edged sword of digital connectivity. It showed its origin, factors contributing to this crime in Nigeria, and the general impacts of cybercrime. It looked at the role of law enforcement in addressing cybercrime. Digital connectivity has significantly reshaped contemporary society, fostering substantial progress in communication, economic growth, and social inclusion. However, as dependence on digital technologies intensifies, the associated vulnerabilities to cyber threats have become increasingly complex and pervasive as cybercriminals are significantly influenced by their social environments such as online forums, dark web communities, and hacker networks, where they acquire technical skills and adopt justifications for engaging in cybercrime. It is therefore essential to establish a sustainable equilibrium between harnessing digital innovation and ensuring comprehensive cybersecurity through a collaborative multi-stakeholder approach encompassing governmental bodies, the private sector, academia, and civil society. Key strategies include the reinforcement of legal and regulatory frameworks, strategic investment in cybersecurity infrastructure, the promotion of digital literacy, and, the facilitation of cross-border cooperation. These measures are critical to preserving the advantages of digital connectivity while effectively mitigating its risks.

References

Adewopo, V. A., et al. (2024). A comprehensive analytical review on cybercrime in West Africa. *arXiv*. https://doi.org/10.48550/arXiv.2402.01649

Ajayi, O., Amorighoye, D. E., & Osayi, M. I. (2025). Root causes of cybercrime among undergraduates in Benin City. *African Journal of Social and Behavioural Sciences, 15*(1).

Akers, R. (2017). *Social learning and social structure: A general theory of crime and deviance*. Routledge. https://doi.org/10.4324/9781315129587

Alabi, A., Bamidele, A. H., & Oladimeji, A. B. (2023). Cybercrime in Nigeria: Social influence affecting the prevention and control. *Lafia Journal of Economics and Management Sciences, 8*, 227–241.

Aldoghmi, H. S. (2024). The role of international efforts in combating cybercrimes. https://doi.org/10.24940/theijhss/2023/v11/i11/hs2311-019

American Psychological Association. (2023). *The emotional toll of identity theft*. https://www.apa.org

Auwal, A. M. (2023). The overview of cybercrime and cyber security in Nigeria and its future trends

Awhefeada, U. V., & Bernice, O. O. (2020). Appraising the laws governing the control of cybercrime in Nigeria. *Journal of Law and Criminal Justice, 8*(1), 30–49.

Babanina, V., Tkachenko, I., Matiushenko, O., & Krutevych, M. (2021). Cybercrime: History of formation, current state and ways of counteraction. *Amazonia Investiga, 10*(38), 113–122.

Borghard, E. D., & Lonergan, S. (2021). The future of cyber conflict: Rethinking cyber warfare strategy. *Strategic Studies Quarterly, 15*(2), 45–67.

Dearden, T. E., & Parti, K. (2021). Cybercrime, differential association, and self-control: Knowledge transmission through online social learning. *American Journal of Criminal Justice, 46*(6), 935–955.

Europol. (2022). *The psychological impact of cybercrime on victims*. https://www.europol.europa.eu

Forrester. (2023). *The future of cybersecurity regulations and compliance costs*. https://www.forrester.com

Gartner. (2022). *AI and machine learning in cybersecurity: Market trends*. https://www.gartner.com

Holt, T. J. (2019). *The human factor of cybercrime*. Routledge.

IBM. (2023). *Cost of a data breach report 2023*. https://www.ibm.com/security/data-breach

Ibrahim, Y. A., et al. (2024, April). Cybersecurity and cybercrimes in Nigeria: An overview of challenges and prospects. In *Proceedings of the 2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG)* (pp. 1–7).

Leenen, L., Van Vuuren, J., & Van Vuuren, A. J. (2020). Cybersecurity and cybercrime combatting culture for African police services. In *International Conference on Human Centered Computing*. https://doi.org/10.1007/978-3-030-62803-1_20

Makeri, A. Y. (2017). Cyber security issues in Nigeria and challenges. *International Journal of Advanced Research in Computer Science and Software Engineering, 7*(4).

Marcelino, A. (2022). Understanding the types of cybercrime and its prevention. *Mathematical Statistician and Engineering Applications, 71*(1), 108–112.

Miller, B., & Morris, R. G. (2016). Virtual peer effects in social learning theory. *Crime & Delinquency, 62*(12), 1543–1569.

Odesanmi, A., et al. (2023, April). Effects of contraceptives non-use on sexual engagement among secondary school students in North Central, Nigeria. In *2023 International Conference on Science, Engineering and Business for Sustainable Development Goals (SEB-SDG)* (Vol. 1, pp. 1–9).

Schjolberg, S. (2020). *The history of cybercrime* (Vol. 13). BoD–Books on Demand.

Sousa-Silva, R. (2024). We attempted to deliver your package: Forensic translation in the fight against cross-border cybercrime. *International Journal for the Semiotics of Law*. https://doi.org/10.1007/s11196-023-10102-2

Sutardi, S., & Ferdiles, L. (2023). Law enforcement against cybercrime in online activities. *Edunity Kajian Ilmu Sosial dan Pendidikan, 2*(1), 38–46.

Urhibo, K. (2021). Combating and addressing the menace of cybercrime in Nigeria: An overview of applicable laws. *African Journal of Criminal Law and Jurisprudence, 6*, 109.

U.S. Senate Intelligence Committee. (2020). *Russian cyber interference in the 2016 U.S. election*. https://www.intelligence.senate.gov

Verizon. (2023). *Data breach investigations report: Impact on SMEs*. https://www.verizon.com/business/resources/reports/dbir