African Journal of Social and Behavioural Sciences (AJSBS)
Volume 16, Number 2 (2026) ISSN: 2141-209X

# THE EFFECTS OF CYBERCRIME ON NIGERIA'S NATIONAL SECURITY: EVIDENCE FROM GOMBE STATE, NORTH-EASTERN NIGERIA

**Usman Ahmed[1]* & Yusuf Nabil[2]**

[1]Department of International Relations, Federal University of Kashere, Gombe State, Nigeria

[2]Department of Political Science, Federal University of Kashere, Gombe State, Nigeria

*uothmasan01@fukashere.edu.ng

**ABSTRACT:** Cybercrime encompasses a wide range of illegal activities, including online fraud, identity theft, hacking, cyber espionage, misinformation and cyber-attacks against individuals, businesses, and government institutions. The challenges posed by cybercrime to Nigeria's national security are indeed worrisome and thus call for concerted efforts of the major stakeholders across the government agencies. The menace is so obvious that it enormously affects Nigeria's national security. The study adopts a qualitative research method utilising both primary and secondary sources of data. The primary data were obtained through key informant interviews with fourteen (14) persons purposively selected from relevant agencies and institutions involved in cybercrime and national security. The documentary analysis was equally utilized to augment data obtained from the key informant interview in order to ascertain the validity and reliability of the data collected. The secondary data consist of books, journals, and internet sources. Digital Ecosystem Vulnerability Theory was utilized as a theoretical framework. The study findings reveal that cybercrime is increasing rapidly in Nigeria undetected, affecting its critical national infrastructure, causing prolonged terrorism, and affecting national security. The study recommends that raising public awareness about cyber security risks and best practices ensuring adequate funding for cyber security initiatives, fostering robust partnerships between the government, private sector, and civil society organizations and by uniting these sectors, Nigeria can build a more resilient and secure digital environment that not only protects the country's digital assets but also lays solid foundation for a safer digital future.

**Keywords:** Cybercrime, Cybersecurity, Cyberspace, Security, National-Security

## INTRODUCTION

The growing increase of global interdependence on Information and Communication Technology (ICT) has positively impacted political, economic, and social systems across the world. Thus, ICT has enhanced efficiency in global governance and economic growth, but it has also increased the spate of cybercrime activities within the existing global digital platforms. Cybercrime encompasses a wide range of illegal activities such as online fraud, identity theft, hacking, cyber espionage, misinformation, and cyber-attacks against individuals, businesses, and government institutions. Das and Nayak (2013) describe cybercrime as offences in which computers and networks serve as tools or targets posing significant risks to the security and stability of nations. Similarly, Muraina and

Muraina (2015) argue that, cybercrime involves deliberate attempts to harm or defame individuals or groups through digital communication platforms such as social media and mobile networks. These activities have increasingly threatened state authority, public trust, and institutional integrity. Cybercrime therefore, has been construed as offences committed against computer data, computer data storage media, computer systems and service providers (Massawe and Mshana, 2023).

Globally, cybercrime has become one of the fastest growing forms of crime, largely due to the anonymity and borderless nature of cyberspace (Smith & Perry, 2021). Caravelli (2019) notes that cybercrime now ranges from social attacks such as cyber bullying and the spread of disinformation to sophisticated intrusions targeting government agencies and critical infrastructure. Smith and Perry (2021) estimate global cybercrime losses at over $5.2 trillion between 2019 and 2023, while global cyber security spending exceeded $1 trillion between 2017 and 2021. The COVID-19 pandemic further facilitated dependence on digital platforms, shifting governance, commerce, and social interaction online and elevating cyber threats to a core national security concern (Smith & Perry, 2021).

Africa has experienced a rapid increase in internet penetration, rising from 2.1% in 2005 to 24.4% in 2018, thereby increasing exposure to cyber threats (Bourdillon, 2023). According to Kshetri (2013), an internet penetration rate of 10–15% often marks the threshold for significant hacking activity, a level now exceeded by many African countries. As a result, cybercriminals increasingly target African states, viewing them as "low-hanging fruit" due to weak cyber security frameworks and limited technical capacity (Kshetri, 2019). In 2017 alone, cyber-attacks reportedly cost African economies approximately $3.5 billion, with Nigeria accounting for about $649 million of these losses (Kshetri, 2019).

In Nigeria, cybercrime has evolved from isolated financial fraud to a broader national security threat. Cyber-attacks on financial institutions, telecommunications networks, and government databases have exposed sensitive information and weakened public confidence in state institutions (Ibrahim, 2016; Akande & Bello, 2019). The Nigerian Communications Commission reported cybercrime-related losses of approximately ₦127 billion in 2019, highlighting the scale of the problem (Akande & Bello, 2019). Beyond financial losses, cybercrime has facilitated identity theft, espionage, sabotage, and the manipulation of public opinion, all of which pose serious risks to national security.

Cyber threats in Nigeria also manifest through misinformation and digital propaganda. Lukman and Monsuru (2020) document how false reports concerning President Muhammadu Buhari's alleged death in 2018 circulated widely on social media, undermining public trust and social stability. Similarly, social media platforms, particularly Twitter, played a central role in mobilizing the End SARS protests in 2020, demonstrating how cyberspace can be used to challenge state authority and escalate internal security tensions. Furthermore, reports of widespread cyber-attacks during the 2023 general elections underscore the vulnerability of Nigeria's democratic processes to cyber interference.

Another major national security concern is the centralization of citizens' data through initiatives such as the National Identity Number (NIN) and Bank Verification Number (BVN). While these

initiatives were designed to enhance governance and security, they have also increased the risk of large-scale data breaches, exposing both citizens and the state to cyber exploitation. Cybercriminals have reportedly used stolen identities to register SIM cards, launder money, and coordinate criminal and insurgent activities, including operations linked to Boko Haram, thereby undermining national security and surveillance efforts (Akande & Bello, 2020). The cases of cybercrime victimization in Nigeria are rapidly increasing day by day, with the expansion of digital cyberspace like social media platforms (Facebook, Twitter WhatsApps), mobile networks (Apple, Samsung, Nokia, Huawei), supermarkets (Amazon, Ali Baba, Ali Express, Temu) and financial networks such as banks and stock exchanges. This growth in digital interaction created opportunities for criminals.

Despite efforts by the Nigerian government to combat cybercrime through legislation, surveillance, and public awareness campaigns, cyber insecurity remains pervasive. Studies have identified key challenges such as inadequate cybersecurity infrastructure, shortage of skilled cybersecurity personnel, weak enforcement of cyber laws, insufficient funding, and low levels of digital literacy among citizens and institutions (Adeshina et al., 2019; Suleiman, 2019; Mustapha & Ismail, 2019; Akpan, 2019; Michael & Mathias, 2019; Kshetri, 2019; Oluwatayo et al., 2020; Ezekiel et al., 2021; Adetiba & Adewale, 2021; Sule et al., 2022; Bourdillon, 2023; Usman et al., 2023).

Thus, the persistence of cybercrime in Nigeria raises critical questions about what went wrong in the country's national security architecture. The failure to effectively secure cyberspace has compromised governance, social stability, and public confidence in state institutions. It is against this backdrop that this study examines cybercrime and national security in Nigeria, with the aim of identifying systemic weaknesses and explaining why existing measures have been insufficient in addressing the growing cyber threat.

## Conceptual Clarifications of Key Terms

### The concept of Cybercrime

Cybercrime has become a persistent and evolving phenomenon since the emergence of the internet, adapting continuously to technological advancement and changing socio-political conditions. Ali (2022) posits that increasing global interconnectedness and overreliance on digital platforms have facilitated the expansion of the scope and sophistication of computer-related crimes. In pre-modern periods, computer crime was largely restricted to individuals with specialized technical access and expertise (Ezekiel et al., 2021). However, the widespread diffusion of digital technologies has lowered entry barriers, making cyber tools easily accessible to both offenders and victims (Pande, 2017). This transformation has shifted cybercrime from isolated acts of data manipulation to large-scale financial, political, and security-related crimes with direct implications for national security.

Cybercrime is not an isolated or independent concept but a collective term describing a wide range of criminal activities linked to computers, networks, and the internet (Lukman & Monsuru, 2020). The increasing use of cyber related terminologies such as cyber security, cyber terrorism, cyber espionage, cyber economy, and cyberspace reflects the growing centrality of digital systems to modern governance and security architecture (Lukman & Monsuru, 2020). According to Ezinne (2022), the term "cyber" originates from cybernetics and refers to interactions involving computer

systems and digital networks. When combined with crime defined as harmful acts or omissions legally prohibited because they threaten public welfare and moral order (Ezinne, 2020) cybercrime emerges as a specialised form of criminality carried out through digital means.

Several scholars have defined cybercrime in ways that underscore its relevance to national security. Ezinne (2020) and Ibrahim (2019) describe cybercrime as the use of computers and the internet by technically skilled individuals to commit illegal acts. Maitammi (2013) further explains that cybercrime involves the exploitation of computer systems and online platforms to target government data, corporate organizations, and individuals. Pande (2017) offers a more comprehensive definition, describing cybercrime as unlawful activities in which computing devices such as smartphones, tablets, and networked systems serve as tools or targets of criminal actions, often driven by motives such as greed, revenge, political interest, or ideological extremism. These broader definitions are particularly relevant to national security, as they capture cyber activities capable of undermining state institutions, critical infrastructure, and public trust.

Das and Nayak (2013) conceptualised cybercrime as offences committed by individuals or organised groups that use computers or networks as tools, targets, or environments for criminal activity, including denial-of-service attacks and system intrusions. Similarly, Muraina and Muraina (2015) view cybercrime as offences commited through modern telecommunications networks to harm individuals or groups psychologically, socially, or reputationally. Synthesising these perspectives, cybercrime can be understood as illegal activities conducted through digital platforms, including online fraud, identity theft, phishing, hacking, cyber espionage, and cyber terrorism many of which directly threaten national security when directed at government institutions and critical infrastructure.

Caravelli (2019) highlights the diverse forms of cybercrime, ranging from social cyber activities such as cyberbullying, online intimidation, and the circulation of explicit materials to sophisticated cyberattacks targeting government agencies and private-sector organizations. Ezinne (2022) categorizes cybercrime into crimes against individuals, crimes against businesses and organizations, and crimes against government. Crimes against the government, such as attacks on national databases, electoral systems, financial infrastructure and security networks pose the gravest threat to national security, as they compromise sovereignty, intelligence, and public order.

Pande (2017) further classifies cybercrime into internal and external attacks, as well as structured and unstructured attacks. Internal or insider attacks are carried out by individuals with authorised access to systems, often motivated by greed or revenge, making them particularly dangerous to national security due to their familiarity with institutional vulnerabilities. External attacks, on the other hand, are executed by outsiders or foreign actors and can result in financial losses, reputational damage, espionage, and sabotage. Structured attacks are usually conducted by highly skilled actors, including professional criminals, terrorist groups, political rivals, or even hostile states, often with clear political or strategic objectives. Such attacks directly intersect with issues of cyber warfare, cyber terrorism, and national defense.

However, Maitammi (2013) and Kshetri (2013) identified some examples of cybercrime which include denial of service attacks, cyber theft, phishing, cyber trespass, attacks on critical

infrastructure, identity fraud, cyber terrorism, cyber extortion, online money laundering, advance fee fraud (419), spamming, and online pornography. These crimes have increasingly been exploited by criminal networks, insurgent groups, and foreign actors to destabilise states, fund terrorism, launder illicit proceeds, and manipulate public perception (Caravelli & Jones, 2019). In Nigeria, such activities have exposed systemic weaknesses in cyber security governance, intelligence coordination, and digital resilience.

Thus, the evolving nature of cybercrime and its increasing sophistication reveal what went wrong in Nigeria's national security framework. Factors such as low digital literacy, weak institutional capacity, inadequate cyber security infrastructure, political instability, and the misuse of new media have created fertile ground for cyber threats to thrive. Cybercrime has therefore moved beyond economic crime to become a strategic national security challenge, capable of undermining governance, social stability, and state sovereignty if not effectively addressed.

**The Concept of National Security**

National security means the total capabilities of state to protect and preserve its vital interest, sovereignty and stability. There has been a global pattern and rise of national security exhibited by different states globally. The nation state is the entity responsible for the personal and collective safety and security of its citizens (Tabansky, 2012). Lukman and Monsuru, (2020) asserted that before the advent of the internet, national security covered only four domains, which are land, sea, air, and space. The triumph of internet aroused the need for national governments to protect their respective cyberspace from cyber-attacks often staged by known adversaries searching for classified information of other states for strategic needs.

Grabosky (2013), also opined that national security is a term used lightly for many reasons, not all of them are legitimate. Traditionally, national security means the capability to deter or to resist the invasion of one's territorial boundaries by foreign military, naval or air forces. Presently, the concept has expanded to embrace a range of factors that might support this capability, including territorial threats to public health, education, welfare, social cohesion and to the national economy. National security is not only the objectives to be achieved, but should be enlightened appropriately to the possible way (Ibrahim *et'al,* 2021). National security should be tightened as the technology nowadays can be reached easily, especially by those attackers, and the government must ensure their security is tightened as technology is moving forward (Ibrahim et'al*,* 2021). In another vein, the national security policy of any state must describe challenges internally and externally and address them accordingly before interacting on the global level, (Sule et'al, 2021).

National security covers the various measures and strategies deployed by a state to safeguard its citizens, territorial integrity, economy, critical infrastructure and institutions from threat, both internal and external, (Njoko & Amoo, 2021). Such protection might be employed by military or non-military human security, economic protection of states, political, social and state valuable interest from threats. In contemporary times, national security entails the protection of a country's digital space from cyber-attacks emanating from internal or external sources, which might undermine, erode and thereby threaten the survival of the state as a nation (Bobade., 2017).

Additionally, Sule et'al, (2021), opined that the present-day national security must address more than just military threats, including climate change social settings, political structure, and the economic basis of the country, among others where cyber security is prominent among them, thus with over-reliance on ICT, cyber-attacks have become critical concerns for national security. Cyber warfare has brought an impact on national security when national security is weakened and can easily be hacked by those attackers and manipulate the sensitive government data, ((Ibrahim et'al, 2021).

Cybercrime continues to grow rapidly and challenges developed nations in different ways (Tabansky, 2012). It causes many kinds of damage to citizens and organizations. According to National Cyber Security policy (2014), cyber space has become an indispensable global domain coming after land, sea, air, and space as number five. Increasingly, nations are depending on ICT infrastructure in governing societies, conducting business, exercising individual rights in interactions and freedom of communication.

Cyber war would have appeared as a myth to many. Still, occurrences in the cyberspace between powerful actors in America, Eastern Europe, Africa Asia and other regions of the world proved the realness of cyber war as a threat to internal and external sovereignty of states, especially to digital infrastructures which characterized the economic and political strengths of countries, (Lukman & Monsuru, 2020).

Caravelli (2019), provided various instances in which cybercrime influences political events in different countries. Russia was allegedly involved in cyber-attacks against the United States during the 2016 presidential election. President Obama took retaliatory actions, including the expulsion of Russian operatives, imposition of sanctions, and closure of Russian compounds. Russia retaliated by expelling U.S. embassy staff. German officials suspected Russian involvement in cyber-attacks targeting government officials and political parties. However, the German election in 2017 was not heavily targeted due to preparations and defense measures (Caravelli, 2019). Russian hackers targeted France's TV5 Monde and engaged in disinformation campaigns during the 2017 national election, supporting Marine Le Pen, although Emmanuel Macron won the presidency. Numerous cybercrime attempts were scrutinized in relation to the Brexit vote. Twitter accounts were found to have posted messages supporting Britain's exit from the European Union. The use of social media for illicit purposes, such as spreading disinformation, raises questions about the integrity and credibility of these platforms (Caravelli, 2019). Social media played a crucial role during the Arab Spring in Egypt, enabling protests against President Hosni Mubarak's rule (Caravelli, 2019). Similarly, social media, particularly Twitter, fueled the End SARS protest 2020 in Nigeria, with the sole aim of causing revolution in the state. Addressing the menace of cybercrime is crucial for safeguarding the nation's national security

According to Tabansky (2012), the escalation of cybercrime activities such as theft and industrial espionage, fraud, harmful contents, hate crime, destruction of websites, denial of service, and so on, posed a great danger to national security. The state must upgrade its involvement in creating cyberspace security, but it cannot solve the problem alone. The successful realization of state responsibility for cyberspace security necessitates the cooperation of all interested parties in the business, academic, public, and security sectors, so as to provide national and personal cyberspace

security to the state and its citizens (Tabansky, 2012). Addressing the menace of cybercrime is crucial for safeguarding the national security of a state.

**Cybercrime and National Security in Nigeria**

Africa has experienced rapid digital growth, with internet penetration rising from 2.1% in 2005 to 24.4% in 2018 (Bourdillon, 2023). Nigeria's digital expansion is significant, with a population of 221.2 million in 2023, of which 87.7% have mobile phone connections and 55.4% are internet users (Digital 2023: Nigeria). This increased digital access has created a fertile ground for the growth of the digital economy but also exposes the country to rising cybercrime threats that impact national security (Bourdillon, 2023).

The Nigerian digital economy, encompassing e-commerce, e-governance, online banking and other digital initiatives accounted for 17.8% of Nigeria's GDP in 2020 (NBS, 2021). However, cybercrime incidents have threatened the stability, trust, and growth potential of this sector. The sensitivity of Nigeria's digital infrastructure and data makes it vulnerable to cyber threats that can compromise critical systems and disrupt essential services (Ojo et al., 2020).

Cybercrime undermines data privacy and personal security, leading to identity theft and online exploitation. Such breaches have severe emotional, financial, and social consequences that erode trust in digital platforms, thereby negatively affecting Nigeria's national security and digital economy (Ajayi, 2016; Ukwuoma et al., 2022). This erosion of trust extends to individuals, businesses, and government institutions, complicating effective governance and social order (Akande & Tsoho, 2021).

Furthermore, cyber-attacks on critical infrastructure, including telecommunications networks, power grids and financial systems, can cause widespread disruption, economic losses, and social unrest (Asogwa et al., 2020). Given the interconnectedness of digital systems, government institutions and national defense systems are particularly vulnerable to cyber intrusions, which can lead to unauthorized access, theft of sensitive information, and disruption of essential services (Dike et al., 2020; Njoku & Amoo, 2021).

The consequences of these cyber-attacks pose significant risks to data integrity, intellectual property, public safety, and national sovereignty (Ojo et al., 2020). Therefore, addressing cybercrime is critical to safeguarding Nigeria's national security and fostering the continued growth of its digital economy.

**Theoretical Framework**

The study adopts Digital Ecosystem Vulnerability Theory as a framework. The Digital Ecosystem Vulnerability Theory is premised on the dynamic interconnected nature of digital ecosystems, in which vulnerabilities continuously emerge due to rapid technological advancements, software and hardware interdependence, and the inherent difficulty of securing every component in complex digital systems. As digital ecosystems expand, they become increasingly exposed to cyber threats that can undermine economic stability, governance, and national security.

This theory draws from extensive scholarship in cyber security, computer science, network systems, and social theory. Key contributors include Castells (1996), Buchanan (2002), Barabási (2003), Clarke (2013), Weißhuhn, Müller and Wiggering (2018), Lippert and Cloutier (2021), and Kang et al. (2022). These scholars collectively explain how vulnerabilities manifest, diffuse, and intensify within interconnected systems, making them susceptible to both internal and external threats such as cybercrime and cyber terrorism.

Ecological vulnerability from which this theory is adapted, refers to the degree of system disturbance, damage, and capacity for recovery (Kang et al., 2022). Vulnerability analysis focuses on identifying weaknesses within a system that can be exploited by threats capable of causing significant harm (Wisner et al., 2004, cited in Weißhuhn et al., 2018).

In the context of cyberspace, a digital ecosystem comprises stakeholders, digital infrastructure, institutions, and enabling environments that allow individuals, organizations, and states to access services, interact, and pursue economic opportunities (UN, 2021). While data and digital technologies offer immense developmental benefits, their misuse or inadequate protection exposes states to cybercrime, espionage, and cyber warfare. These vulnerabilities become particularly dangerous when they affect critical infrastructure, financial systems, electoral processes, and government databases, thereby posing direct threats to national security.

The proponents of the Digital Ecosystem Vulnerability Theory argue that technology creates a constantly evolving system with interdependent components, each influencing political authority, economic performance, and social order. As the digital ecosystem expands through social media platforms, mobile networks, e-commerce systems, and financial technologies, it simultaneously creates new vulnerabilities, including cybercrime, cyberterrorism, economic disruption, and governance challenges. This makes cooperative governance, adaptive regulation, and coordinated cyber security strategies essential.

In Nigeria, rapid digital adoption between 2019 and 2023, particularly in e-governance, online banking, social media use and e-commerce, has increased exposure to cyber threats such as phishing, identity theft, cyber fraud, disinformation, misinformation and attacks on government systems. These threats undermine public trust, weaken institutional authority, disrupt economic activities, and threaten national stability. The Digital Ecosystem Vulnerability Theory, therefore, provides an appropriate framework for understanding how cybercrime exploits systemic weaknesses within Nigeria's digital environment to challenge national security.

The Digital Ecosystem Vulnerability Theory is relevant to this study because it explains how accelerated digitalization heightens exposure to cyber threats that affect national security. It provides insight into how cybercrime exploits systemic vulnerabilities arising from weak regulation, inadequate cyber security infrastructure, and uneven digital literacy.

The theory also helps in analyzing government and international responses to cyber threats, including legislation, policy frameworks, and institutional reforms aimed at securing Nigeria's cyberspace. It is particularly useful in examining how cybercrime during the 2019--2023 period affected e-government initiatives, electoral integrity, financial systems, and national cohesion.

Unlike previous studies that relied on frameworks such as Social Strain Theory, Routine Activity Theory, Securitization Theory, or Realist approaches, this study introduces the Digital Ecosystem Vulnerability Theory as a more holistic framework that integrates cyber security, digital economy, and national security perspectives.

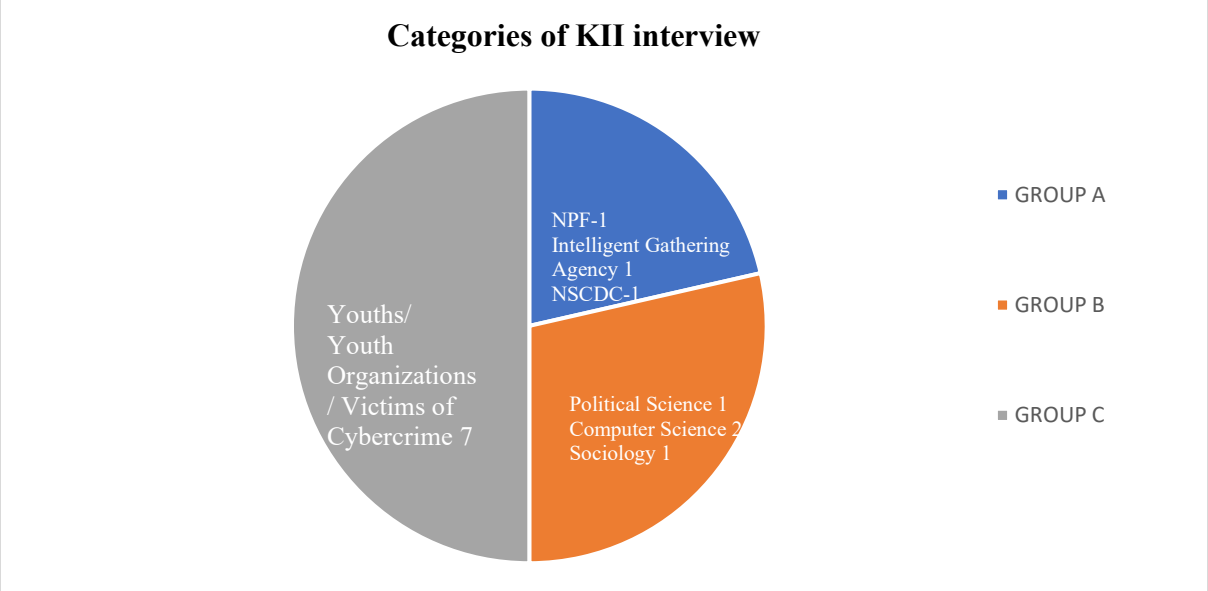
Ultimately, the theory enables an understanding of whether cyberspace becomes a source of conflict or stability, emphasizing the need for resilience, adaptive capacity, and coordinated cyber governance. Its assumptions are relevant and accessible, offering a strong analytical lens for examining cybercrime as an emerging national security threat in Nigeria and across Africa.

## RESEARCH METHODOLOGY

The study uses both primary and secondary sources of data. For the secondary source, information was drawn from books, journals, articles, newspapers, magazines, as well as other internet sources, print media, and written reports from agencies, departments and ministries concerned within and outside Gombe State. Relevant reports, cyber security frameworks, and legislative documents were also analyzed to gain insights into existing policies, challenges, and trends in addressing cybercrime within the Nigerian context. The primary data were obtained through semi-structured interview with the concerned agencies. The study employed the use of In-depth interviews with key stakeholders, including cyber security experts, law enforcement officials, and industry leaders. A semi-structured interview guide was developed, allowing for flexibility while ensuring that key topics related to the effect of cybercrime on national security are covered. This is to have a diverse group that can provide meaningful and varied perspectives on the topic. This approach enables the extraction of rich, qualitative data from participants. Key informant interviews were conducted among fourteen (14) purposively selected stakeholders in order to have valid and accurate information. This was informed by nature of the study which requires sensitive information. It on this note that only few strategic personnel are required. In the first category, a senior police officer was selected and interviewed from the department of cybercrime who is in charge of cybercriminal acts, then, the head of intelligent department from Intelligent Gathering Agency was interviewed and he was responsible for overseeing issues concerning cyber space and cybercrime and lastly, one senior officer, from the Nigerian Security and Civil Defense Corps. The second category comprises mainly of academics from whom four were purposively selected from Gombe state university based on the proximities of the researcher. The first was chosen from the department of political science with specialization in Political economy, two from the department of computer science with specialization in cyber security, and the last one from the department of sociology with specialization in criminology. Then the third category comprises of seven (7) youths who have experiences in ICT, Cryptocurrency, and victims of cybercrime.

Below is the chart-scores representation of the interviewees indicating their numbers and groups or categories.

Figure 1: Categorization and number of respondents under each category.




**GROUP A** = $^{3}/_{14} \times 360 = 77.1$

**GROUP B** = $^{4}/_{14} \times 360 = 102.6$

**GROUP C** = $^{7}/_{14} \times 360 = 180$

**TOTAL:** 360

From Figure 1 above, Group A has a score of 77.1, comprising the NPF, the Intelligent Gathering Agency, and the NSCDC. The group consists mainly of Nigerian law enforcement and security agencies. Group B, which also has a 102.6 score, comprises mainly academicians in the Political Science, Sociology and Computer Science Departments of the Gombe State University. Lastly, Group C, which has a 180 score, comprises youths with experience in ICT, cryptocurrency business, and as victims of cybercrime. The interview responses were collated, coded and analyzed thematically.

## RESULTS

### The nature of Cybercrime in Nigeria

The following were identified in the course of the interview as the nature of cybercrime in Nigeria: Identity theft, Character Deformation, Online Fraud and Phishing. Thus, based on the responses gathered, identity theft presents the most prevalent nature of cybercrime in Nigeria and is closely followed by online fraud, phishing and character deformation. The reports of EFCC convictions of 2021 and 2022 have further shown that identity theft and online fraud are the most prevalent cybercrimes in Gombe State. Moreso, the Gombe state police has affirmed that within the period

under study, online banking fraud and identity theft are the most prevalent cybercrime in the state, stating that its crime unit has investigated 788 cases of such crime. The officer interviewed finally asserts that most of the cases of cybercrime are not being duly reported in the state. Consequently, the nature of interdependence explains why individuals and institutions are susceptible to identity theft and online fraud vulnerability.

**How does cybercrime manifest in Nigeria's national security?**

The following were identified as the manifestations of cybercrime in Nigeria: Threat to individual security, Data destruction and Technological Advancement. Thus, cybercrime significantly affects Nigeria's national security, primarily through data destruction as gathered from the Nigerian Police force, a security expert, a senior lecturer from the political science department of Gombe State University and a Senior Computer system analyst. Similarly, threats to individual security are equally an area of cybercrime identified by the respondents as the second area of manifestation in Nigeria. These findings indicate that cybercriminal activities frequently lead to the loss or compromise of critical data, disrupting governmental and financial operations while jeopardizing the safety and privacy of citizens through identity theft and online fraud.

**Ways in which identity theft affects the national security of Nigeria**

Financial fraud, Terrorism and Trust erosion are the three ways identified as the most frequent ways in which identity theft affects Nigeria's national security. The interviewed conducted among the Nigeria Police Force, Victims of cybercrime, Nigerian security and civil defense corps, Intelligent Gathering Agency, Security expert, a Lecturer 1 from Computer science department of the Gombe state University revealed that financial fraud facilitated by identity theft, leads to unauthorized access to bank accounts and credit card misuse, resulting in significant monetary losses that undermine the stability of Nigeria's financial system. The most critical impact is the erosion of trust, as compromised personal information diminishes citizens' confidence in the government's ability to protect their privacy and security, thereby hindering online engagement and economic growth. Additionally, identity theft can facilitate terrorist activities by providing criminals with false identities to evade detection and plan attacks. The cases highlighted in the EFCC reports and the Global Cyber security Index further support these findings, pointing to substantial fraud costs, especially within the banking and digital financial sectors.

**Effectiveness of the laws tackling the prevalence of cybercrime in Nigeria**

The interviews conducted among the relevant stakeholders indicate that Nigeria's laws tackling cybercrime are deemed fairly Effective. This is due to the high-rising challenges posed by cybercrime in Nigeria. Also, the application of law itself in many instances is selective in nature. This largely undermining the sanctity of the institutions saddled with such responsibility and this also explains the weak nature of the institutions.

**Challenges associated with cyber security in Nigeria**

The interviews conducted among the identified stakeholders on cybersecurity show that Lack of awareness and education, Lack of effective cyber law, Political corruption and Lack of funding are the major challenges confronting Nigeria's cybersecurity. These challenges indeed affect the country's ability to protect its digital economy and national security. The interviews with the Nigerian police force and Nigerian civil defense cops validate this, that among all the cybercrime cases reported in the state, only a few were investigated and prosecuted, while many were hanging in the court of law because of political corruption.

**Measures for tackling the scourge of cybercrime in Nigeria**

To effectively tackle the cybercrime menace in Nigeria, a multi-dimensional approach that incorporates awareness, training and legal frameworks was suggested by the interviewees. This multidimensional approach might be attributed to the complex nature of Nigeria and its institutions. Suggesting on how to combat the scourge of cybercrime in Nigeria, increasing awareness about the threat of cybercrime becomes necessary. Also, improving equipment and training for enforcement agencies, as well as strengthening legal frameworks, are equally necessary.

**Conclusion and Recommendations**

Conclusively, the study establishes that cybercrime in Nigeria is predominantly driven by identity theft, online fraud, phishing, and impersonation on digital spaces, all of which pose serious threats to national security. These crimes compromise sensitive data, weaken public trust, disrupt financial systems, and create opportunities for criminal and terrorist activities. The persistence of cybercrime in Nigeria reflects deeper institutional weaknesses, including ineffective enforcement of cyber laws, limited public awareness, political interference, and inadequate investment in cyber security infrastructure.

It is further demonstrated that national security in the digital age extends beyond military defense to include the protection of data, financial systems, and citizen trust. Without decisive reforms in cyber security governance, public education, legal enforcement, and reporting mechanisms, cybercrime will continue to undermine Nigeria’s security and development objectives.

To ameliorate the effects of cybercrime on Nigeria’s national security this study recommends that a comprehensive national cyber security strategy should be developed to provide a coordinated and cohesive framework for preventing, detecting, and responding to cyber threats at the national level. This strategy should be complemented by the establishment of a specialized cyber security agency dedicated solely to the identification, investigation, and prevention of cybercrime across the country.

In addition, the study recommends the development of a nationally accessible cybercrime reporting application to enable all Nigerians to easily and confidentially report cybercrime incidents. This is particularly important given the finding that many cybercrime cases remain unreported, thereby weakening national security intelligence and policy responses. The government should also allocate

adequate funding and resources to strengthen cyber security infrastructure, enhance digital forensic capabilities, and support continuous training of security personnel.

Furthermore, integrating cyber security education and digital literacy into school curricula at all levels would magnanimously improve public awareness and equip future generations with the skills required to safely navigate digital spaces. Finally, strengthening international cooperation is essential for combating transnational cybercrime, as many cyber threats originate beyond national borders. These measures would enhance Nigeria's national security, protect its digital economy, and foster a safer, more resilient digital environment capable of supporting sustainable technological and economic growth.

**REFERENCE**

Adeshina, O. O., Uzor, S. C., & Rannat, A. B. (2019). Cybersecurity governance in Nigeria: A review of policies, frameworks, and challenges. *Information Security Journal: A Global Perspective*, 28(1–3), 72–82.

Adetiba, E., & Adewale, O. S. (2021). Cybersecurity threats and impediments to innovation in Nigeria's digital economy. In Proceedings of the 3rd International Conference on Information Technology and Digital Applications (pp. 95–102).

Ajala, T. A., Chukwu, F., & Afolabi, I. T. (2020). Cyber security challenges in Nigeria: A systematic review. *Journal of Information Privacy and Security, 16(3), 181–194*.

Ajayi, E. (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet Information Systems, 1(6), 1–12. https://doi.org/10.5897/jiis2015.0089*

Akande, F., & Bello, I. (2019). Cyber threats and national security: A case study of Nigeria. *International Journal of Security and Defense Studies, 15(3), 200–215.*

Akande, J. O., & Tsoho, A. U. (2021). The implications of cybercrime on e-commerce and national security in Nigeria. *Journal of Internet Technology and Information Security, 12(2), 7–19.*

Akpan, E. E. (2019). Strategic assessment of cybercrimes control through cyber security and resilience: The Nigeria experience. Shared Seasoned *International Journal of Library and Information Science, 3(2).*

Ali, I. P. (2022). Cybersecurity initiatives for securing a country. Ibadan: University Press PLC.

Asogwa, B. E., Ezema, I. R., & Ugwoke, C. O. (2020). Cybercrime and national security: An analysis of the Nigerian perspective. In Proceedings of the 2nd International Conference on Science and Sustainable Development (pp. 94–104).

Barabási, A. L. (2003). Linked: The new science of networks. Perseus Publishing.

Bobade, I. Y. (2017). Cyber threats and national security in Nigeria: Challenges and options. NDC Journal, 131–146.

Bourdillon, O. O. (2023). The effect of online fraud on the adoption of digital economy in Nigeria: A review. *African Journal of Management and Business Research, 10(1).*

Buchanana, M., (2002). Small worldinvestigates vulnerabilities in complex networks and the potential for cascading failures.

Nigeria Bureau of Statistics. (2021). Nigerian gross domestic product report: Q4 2020. https://nigerianstat.gov.ng

Caravelli, J., & Jones, N. (2019). Cyber security: Threats and responses for government and business. Praeger Security International.

Castells, M. (1996). The rise of the network society. Blackwell Publishers.

Clarke, R. (2013). A preliminary characterization of information privacy invasion. *Journal of Information Technology, 28(1), 1–12.*

Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (Nigeria). https://cert.gov.ng

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International Journal of Engineering Sciences & Emerging Technologies, 6(2), 142–153.*

Dike, I., Egbetokun, A., Adesida, A., & Olokundun, M. (2020). Cybersecurity threats and national security in Nigeria. *Journal of Contemporary African Studies, 38(1), 88–106.*

Economic and Financial Crimes Commission. (2022). Narrative of convictions. EFCC.

Ezekiel, M., Salihu A. G., and Abdulkarim R., (2021). A Historical Assessment of Cybercrime in Nigeria: Implication for Schools and National Development. *Journal of Research in Humanities and Social Science Volume 9 (9) 84-94.*

Ezinne O.O. (2022). Examining the Effect of the Elevated Rate of Cybercrime on the Growth and Sustainable development of Nigeria's Economy.*NnamdiAzikwe University, Journal of commercial and property law.* Vol. 9 (1) ISSN: 2736-0342.

Federal Bureau of Investigation. (2020). Internet crime report. FBI.

Federal Bureau of Investigation. (2021). Internet crime complaint center report. FBI.

Federal Bureau of Investigation FBI (2018). Internet Crime Report

Grabosky, P. (2013). Organised cybercrime and national security. Chatham House. National University.

Ibrahim, S. (2019). Causes of socioeconomic cybercrime in Nigeria. In IEEE International Conference on Cybercrime and Computer Forensic (pp. 1–9). https://doi.org/10.1109/ICCCF.2016.7740439

Kshetri, N. (2013). Cybersecurity and cybercrime: Issues and solutions in the digital age. Springer.

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management.* https://doi.org/10.1080/1097198X.2019.1603527

Kang H, Wendong T, Dan He &Xuxiang Li (2022) A new perspective on ecological vulnerability and its transformation mechanisms, Ecosystem Health and Sustainability, 8:1, 2115403, DOI: 10.1080/20964129.2022.2115403

Lippert, K.J.; Cloutier, R. (2021), Cyberspace: A Digital Ecosystem. System, 9, 48. https://doi.org/ 10.3390/systems9030048S

Lukman, R.A.A and Monsuru, O.R., Cyber Theatre A Fifth Domain Of International Politics: Africa and the rest of the World in the Cyberspac. *AkdenizHavzasıveAfrikaMedeniyetleriDergisi* 2/2 2020 GÜZ

Maitanmi O., Ogunlere, S., Ayinde S., Adekunle Y., (2013). *The International Journal of Engineering and Science (IJES) Volume 2 (4) 45-51.*

Massawe, E.R. & Mshana, J.A. (2023). Preventing and Combating Cybercrimes: Case of Cybercrimes Investigation Unit of Tanzania Police. *European Journal of Theoretical and Applied Sciences, 1*(5), 1-5. DOI: 10.59324/ejtas.2023.1(5). xx

Michael C., and Mathias, B. (2019). Prevalence of Cybercrimes Among Youths In Onitsha South Local Government Area of Anambra State, Nigeria. *International Journal of Health and Social Inquiry*, Vol. 5, No.1

Muraina, M. B., & Muraina, K. O. (2015). Peer pressure, parental socioeconomic status, and cybercrime habit among undergraduates. International Journal of Technology in Teaching and Learning, 11(1), 50–59.

Mustapha, A. B., & Ismail, S. A. S. (2019). Cybercrime and its effects on trust in e-commerce in Nigeria. International Journal of Advanced Research in Computer Science, 10(3), 80–87.

Dasuki, M. S. (2014). National Cybersecurity Policy. FRN

Nwankwo, C. (2015). Cybercrime in Nigeria: Issues and challenges. *International Journal of Humanities and Social Science Invention, 4(5), 42–49*.

Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M., & Esan, A. O. (2017). Cybercrimes in Nigeria: Analysis, detection and prevention. FUOYE *Journal of Engineering and Technology, 1(1).*

Oluyemi, F., Ndubisi, O. N., Ayo, C., Chidozie, F., Ajayi, L., & Okorie, U. (2015, June). Cyber-attack as a menace to effective governance in Nigeria. In *Proceedings of The 15th European Conference on eGovernment ECEG 2015 University of Portsmouth* (p. 107).

Olufokunbi, K. B., Otekunrin, A. O., &Soremekun, I. O. (2019).Cyber Crime and Implications on Internet Governance in Nigeria.In 2019 International Conference on Cyber Warfare and Security (pp. 143-150).

Oluwatayo, A. A., Olufokunbi, K. B., &Olabiyisi, S. O. (2020). Hacking, Fraud, and Cyber Criminality in Nigeria: A Critical Analysis. In 2020 International Conference on Information Networking (ICOIN) (pp. 500-507).

Pande, J., (2017), Introduction to Cyber Security, (FCS), UttarakhandOpen University, Haldwani-263139.

Sule, B., Bakri, M., Usman, S., Mohammed, K. T., & Muhammad, A. Y. (2021). Cybersecurity and cybercrime in Nigeria: Implications on national security and digital economy. *Journal of Intelligence and Cyber Security.*

Sule, B., Usman, S., & Muhammad, Y. (2022). Countering cybercrimes as a strategy for enhancing sustainable digital economy in Nigeria. *Journal of Financial Crime, 1359–0790.*

Smith, R., & Perry, M. (2021).Fake News and the Convention on Cybercrime.*Athens Journal of Law - Volume 7, Issue 3, 2021 – Pages 335-358.*

Stephen, S. D.,(2016). An appraisal of the legal framework for combating cybercrime in international law.A thesis submitted to the postgraduate school, ahmadubello university, zaria in partial fulfilment of the requirements for the award of the degree of masters of law-llm

Usman S., Sule, B., Misbahu, I.Z., and Marie G. N. (2023). Financial Cybercrimes During COVID-19 Pandemic: The Case of Africa. https://www.researchgate.net/publication/369171541

Tabansky, L. (2012). Cybercrime: A National Security Issue? *Military and Strategic Affairs Volume 4 (3). P 117-136*

Ukwuoma, H., Williams, I., Choji, I. (2022). Digital Economy and CybersecurityIn Nigeria. International *Journal of Innovation in the Digital Economy, 1(13), 1-11. https://doi.org/10.4018/ijide.292489*

UN. (2021). World Public Sector Report 2021: Building an Integrated Approach to the Pursuit of Sustainable Development Goals.

Wright, S. (2017). Mythology of Cyber-Crime—Insecurity & Governance in Cyberspace: Some Critical Perspectives. Springer International Publishing AG 2017 J.M. Ramírez and L.A. García-Segura (eds.), Cyberspace, Advanced Sciences and Technologies for Security Applications, DOI 10.1007/978-3-319-54975-0_13.

Williams, C., et al. (2017). "Exploratory Research in Cybersecurity: A Methodological Framework." *Cybersecurity Journal, 10(1), 56-72.*

Weißhuhn , P., Müller F., Wiggering, H., (2018), Ecosystem Vulnerability Review: Proposal of an Interdisciplinary Ecosystem Assessment Approach, Environmental Management, Received: 21 June 2017 / Accepted: 1 March 2018, https://doi.org/10.1007/s00267-018-1023-8