Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13740477

CYBERCRIME AND CYBERSECURITY IN THE ERA OF E-GOVERNMENT: INTERROGATING THE NIGERIAN STATE

ABDULLAHI UMAR
School of Government, Universiti Utara Malaysia (UUM) Kedah, Malaysia.

HALIMAH ABDUL MANAF
Associate Professor, School of Government, Universiti Utara Malaysia (UUM) Kedah, Malaysia.

Abstract

The rise of Information and Communication Technologies (ICT) has transformed the 21st century into a global village, enhancing government and public service delivery by making information more accessible and cost-effective. However, the proliferation of ICT in government also brings the threat of cybercrime, which poses significant challenges to e-government services and national security, particularly in Nigeria. Although the Internet facilitates free access to information, it is also exploited by cybercriminals, adversely affecting public services and cybersecurity. This study aims to address strategies to mitigate the adverse impacts of cybercrime on cybersecurity within the context of e-government in Nigeria. Grounded in the crime opportunity theory, the research adopts a quantitative approach with a survey design. Primary data were collected from 381 out of 1,190 government employees in Kaduna State using a structured questionnaire and Simple Random Sampling Technique. Data analysis used Multiple Regression with the Statistical Package for the Social Sciences (SPSS) version 26.0 to interpret the collected data and derive meaningful insights. The findings indicate a significant positive relationship between cybersecurity and factors such as capacity building, enhanced funding and resources, modernization of IT systems, and public awareness campaigns. However, the relationship between an established incident response and recovery plan and cybersecurity was found to be positive but not significant. Based on these results, the study recommends continuous staff training, recruitment of skilled personnel, collaboration with cybersecurity experts, and stricter sanctions for cybercriminals. Additionally, it advocates for comprehensive cybercrime legislation to combat online threats effectively.

Keywords: Cybercrime; Cybersecurity, E-government, and National Security, Information and Communication Technology.

INTRODUCTION

The rise of global crime has introduced new criminal actors and reshaped the way nations interact on the world stage, both politically and economically. With the increasing integration of Information and Communication Technology (ICT) into our physical world, traditional crimes have found a new breeding ground online, becoming more widespread and complex (Wu, 2022**).** To effectively counter cyber threats, nations must adopt a proactive stance by anticipating and preventing attacks rather than simply reacting to them this may also involve conducting post-incident analyses to identify patterns and anticipate future threats. (Makri, 2017). The surge in state-sponsored cyberattacks on critical infrastructure jeopardizes essential services and national security (Sean, 2023) to counter this growing threat, Nations must adopt a unified defense strategy integrating cyber, physical, and military resources. (Heikkila, 2018; Brands & Van Doorn, 2022).

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13740477

However, this challenge is ongoing as hackers continuously identify new targets and refine their attack methods to bypass existing cyber defence. Threats of cybersecurity extend beyond individuals to encompass organizations and entire nations. These threats include data breaches, cyber-physical attacks (where physical systems are compromised through digital means), crypto jacking (using stolen computing power to mine cryptocurrency), ransomware attacks on cloud storage systems, and even election hacking. For nations conducting elections, the potential disruption of the voting process through hacking poses a significant danger, far more consequential than the spread of misinformation (Giles, 2018; Birkle et al., 2020).

Many countries in the world like the USA, UK India, and Brazil are struggling to combat the new wave of cybercrime (Sean, 2023). These non-state criminal actors, like tax evaders, drug traffickers, and arms dealers, are becoming increasingly sophisticated in their use of technology. Unfortunately, many governments lack the tools and technology to effectively counter these cybercriminals (Collier et al., 2022; Gottschalk & Hamerton, 2022). Threats are increasing in volume, sophistication, and refinement, and they will not leave anytime soon. The frequent breaches and vulnerabilities in cybersecurity raise questions about the effectiveness of the immense resources poured into this field (Eggers, 2016).

Cybercrime is a global issue impacting countries worldwide, including Nigeria. Its effects profoundly disrupt government agencies, public services, and national security. In the 21st century, cybercrime has emerged as a significant obstacle to effective government operations, targeting individuals, businesses, national infrastructure, and various government sectors. Cybercriminals exploit ICT facilities to undermine e-government services, compromising public safety and hindering efficient service delivery (Oni et al., 2024; Gberevbie et al., 2018).

Also, the increasing development and utilization of ICT in Nigeria, particularly in Kaduna State, has made it easier for different government sectors to provide effective and efficient public services (Agbozo, 2018). Kaduna State, in the twenty-first century, is taking advantage of ICT by providing high-quality, cost-effective public services through access to a pool of readily available data, information, and communication (Oni, Berepubo, Oni & Joshua, 2024; Ogu & Chukwurah, 2023).

However, the increasing development and utilization of ICT presents new and emerging challenges for the Kaduna State government to address (Al Amro, 2016). By providing accessible, timely, and cost-effective access to information, e-government has offered many benefits to the people (Robert & Quadri, 2018). Nevertheless, it has also introduced several issues relating to cybercrimes. Cyber-related crimes against governments are major threats impeding the provision of adequate public services. Unauthorized access to ICT infrastructure, data phishing, electronic fraud, spoofing, reproduction, identity theft, disclosure of e-government information, and denial of service (DoS) are some of the common examples of cybercrimes that affect the e-government services (Michael & Deepamalar, 2017; Miller, Higgins & Lopez, 2013).

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13740477

Additionally, to raise the potential of e-government in Nigeria, it is crucial to also address related issues posed by cybercrime. This includes understanding its causes and effects and implementing measures to mitigate its impact. Despite the importance of cybersecurity, existing research has concentrated mainly on the broader impacts of cybercrime without sufficient focus on e-government contexts (Oni et al., 2024; Gberevbie et al., 2018; Michael & Deepamalar, 2017).

Consequently, the aim of the study is to fill this gap by examining strategies to mitigate cybercrime's adverse effects, enhance cybersecurity, and improve e-government services and public service delivery in Kaduna State. It will explore how cybercrime affects e-government utilization, offering insights into practical measures for ensuring the sustainability and efficiency of digital government services. This study will add to the existing body of knowledge

LITERATURE REVIEW

Cybercrime in Nigeria: Threats and Measures for National Security

Information and communication technology (ICT) and the Internet are experiencing explosive growth in Nigeria and worldwide (Anichebe, 2019) However, this rapid advancement has been accompanied by a surge in cyberattacks. As a result, cybercrime and cybersecurity have become critical national security issues (Chung, & Kim, 2022).

Cybercrime encompasses a range of illegal activities facilitated by computers, including the misuse of technology to violate laws and regulations. (Tao et al., 2021). Arpaci and Aslan (2022) define cybercrime as criminal acts committed against individuals or groups with the malicious intent to cause physical or mental harm. These acts specifically exploit modern communication technologies like the Internet and mobile phones to target victims. Cybercrime encompasses two main categories (Okwum, Micheal & Ugboaja, 2017, cited in Chigozie- Hamerton, 2022). The first involves crimes precisely planned and executed using computer technology. The second category refers to traditional crimes that have been transformed using computers, making them more complex and requiring law enforcement to understand computers to investigate them effectively. Maad and Muhammad (2023) define cybercrime as a broad term encompassing various criminal activities. This includes using computers or computer systems as tools to commit crimes, as targets of attacks, or even as a virtual space where criminal activity takes place. Their definition also incorporates traditional crimes that leverage computers or networks to facilitate illegal actions. Cybercrime poses a severe threat to critical infrastructure, potentially disrupting essential services. Imagine trains being halted, aeroplanes receiving false signals, or military secrets falling into enemy hands within seconds due to a cyberattack. These examples illustrate cybercrime's devastating impact on various sectors of society. Recognizing the significant threat cybercrime poses to national security, governments of various nations are actively working to secure their cyberspace from malicious actors. Cybersecurity refers to the practices and measures to protect computer systems and networks from various threats. This includes safeguarding hardware, software, and data from theft, damage, or unauthorized access. Additionally,

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13740477

cybersecurity aims to prevent systems from being disrupted by misleading commands or denial-of-service attacks (Ofori, Udensi & Ibegbu, 2019). The National Initiative for Security Careers and Studies (NICCS) defines cybersecurity as the actions, processes, or capabilities that protect information and communication systems, along with the data they store, from unauthorized access, modification, misuse, or harm (Vishik, Matsubara & Plonk, 2016, p. 221).

Similarly, Ibikunle and Eweniyi (2018) state that cybersecurity is a comprehensive approach encompassing various tools, strategies, best practices, and advancements. This includes security principles, risk management techniques, training programs, and technological developments. Ultimately, it's about safeguarding the cyber environment, an organization's assets, and clients' information. Cybersecurity can be understood in two ways. First, it's a set of principles, like a rulebook, designed to protect the digital world of cyberspace. Second, it's the practical implementation of those principles. This involves a combination of processes, practices, and technology to safeguard networks, computers, programs, and information from threats like unauthorized access or damage. In the same vein, ensuring the safety of ICT frameworks and their content has become known as cybersecurity. According to Fisher (2016) and Collier et al. (2022), cybersecurity refers to a set of exercises and dangers involving computer or computer networks, related hardware, software devices, and the data they contain and convey, including software and information and different components of cyberspace it is also the State or nature of being shielded from such dangers (Fisher, 2016).

Cybercrime in Nigeria: An Emerging Threat to National Security and Economic Stability

Technological progress has created a situation where criminals can efficiently operate across international borders. Advanced technology empowers criminals to exploit security vulnerabilities and conduct activities from unexpected locations far from their home countries. Developing nations are often breeding grounds for cybercrime due to high levels of corruption, which creates an environment conducive to these security breaches. The Internet facilitates criminal activity by enabling them to launder money through fraudulent transactions (Saini et al., 2012). The FBI's latest Internet Crime Report, released in April 2024, reveals a disturbing trend. While the number of cybercrime complaints filed has not doubled in the past four years, associated losses have skyrocketed. The Bureau's analysis shows a staggering $12.5 billion in losses reported in 2023, a $2 billion increase from the previous year and more than triple the amount reported in 2019 (Sean, 2023). This data suggests a troubling escalation in the financial impact of cybercrime. Although cybercrime complaints surged in 2021 compared to the previous year, financial losses increased by only around $700 million (Sean, 2023). However, a significant jump in losses from 2021 to 2022 indicates that cybercriminals have become more adept at stealing considerable sums per attack (Fard & Verna, 2024).

Similarly, Malaysia is experiencing a surge in cybercrime. Over 20,000 incidents were reported in 2021 alone, resulting in losses exceeding RM560 million (approximately $123 million). Estimates suggest total losses between 2017 and 2021 reached RM2.23 billion

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13740477

($490 million). Data from January to July 2022 indicates a continued rise, with reported cases exceeding 11,367, a significant 61% increase compared to 2016 (Gojsa & Toherdoost, 2024).

In Nigeria, tracking cybercrime was not a significant concern in the early 2000s due to limited internet access. However, online financial scams have increased with the rise of the Internet. The anonymity and ease of communication offered by the Internet have facilitated these criminal activities, posing a severe threat to national security (Ibikunle & Eweniyi, 2018). A report by the Nigerian Communication Commission (NCC) indicates a troubling rise in cybercrime within Nigeria, currently ranked fifth globally, following the UK, USA, Canada, and India. Financial losses due to cybercrime in Nigeria were estimated to be over N270 billion in 2023. Nigeria also holds the sixteenth position for cybercrime prevalence worldwide (Premium Times Nigeria, 2024).

Traditionally, countries have four key domains: land, sea, air, and space. Nigeria, however, recognizes cyberspace as a crucial fifth domain essential for driving national capabilities in various areas, including economic development, business transactions, social interactions, government operations, healthcare, national security, and defense. Cybercrime is identified as a critical threat to cyberspace and a significant challenge to national security and growth. These cyber activities affect risk exposure, resistance, and critical and non-critical infrastructure protection. The severity of cyber threats compels Nigeria to prioritize its cyberspace's comprehensive and strategic security, as these threats have severe consequences for the nation's ability to function and compete globally (Dasuki, 2014).

Since the 1990s, Nigeria has faced a growing wave of cyberattacks, prompting collaborative efforts from government agencies, non-governmental organizations, public sector entities, and non-profit groups. This report identifies four main types of cyber threats in Nigeria: phishing attacks, email-borne attacks, malware, and spam. Malware is particularly concerning as it can disrupt computer networks, while email security threats can make it difficult for employees to access essential company information. The prevalence of phishing attacks, which lure unsuspecting users into divulging critical data, exposes organizations to significant risks if they lack adequate security protocols. Strong data systems and robust cyber and data security legislation adhering to International Organization for Standardization (ISO) guidelines are essential to minimize the risk of damaging data breaches and promote a more secure environment for users and investors (Button, 2022; Gojsa & Toherdoost, 2024).

Cybercrime has a devastating impact on nations, causing significant financial losses similar to those inflicted by terrorism. These attacks force citizens and society to bear unexpected costs. Organizations targeted by cybercriminals can suffer reputational damage, leading to declining customer trust. Additionally, preventing cybercrime can reduce productivity, leading to slower production times, increased overhead costs, and, ultimately, unprofitability. Cybercrime also exposes critical Information and Communication Technology (ICT) systems and networks to vulnerabilities, causing

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13740477

further disruptions and wasted time addressing security breaches (Ibikunle & Eweniyi, 2018).

Navigating Cyber Threats: The Critical Role of Cybersecurity in Nigeria's Technological Advancement

Facing a growing threat from cybercriminals, some countries and international organizations have elevated cybersecurity to a national security priority, reflecting its critical importance. As Nigeria's participation in cyberspace expands, it has unfortunately become a target for cybercriminals experiencing many cybercrime incidents. Nigeria has a well-known reputation for cybercrime, particularly advance-fee fraud (often called 419 or Yahoo scams). This has unfortunately led to widespread suspicion of legitimate online transactions originating from Nigeria, both domestically and internationally (Osho & Onoja, 2015). As reliance on technology increases, so do its vulnerabilities. Much of today's technology remains susceptible to hacking. Public demand for robust cybersecurity measures rises with growing public awareness of cybercrime threats (Talansky, 2012; Cerrudo, 2017). Cybersecurity plays a critical role in protecting the global system in today's interconnected world. It extends beyond securing cyberspace and digital information to safeguarding physical structures and security systems, ensuring the overall well-being of our critical infrastructure (Ofori et al., 2017).

Nigeria's economic prominence in Africa underscores the critical need for robust cybersecurity measures. As the nation expands its digital footprint, safeguarding against cyberattacks becomes paramount to maintaining its competitive edge and protecting its citizens (Turianskyi, 2022). Strong cybersecurity practices are essential for protecting businesses and organizations in Nigeria (Bada et al, 2019). This need arises from our increasing dependence on technology, including computer systems, the Internet, wireless networks (like Wi-Fi and Bluetooth), and the ever-growing number of smart devices connected through the Internet of Things (IoT) (Gojsar &Toherdoost, 2024).

The breakneck pace of technological advancement creates a double-edged sword. While it offers exciting possibilities, it also opens doors for new security threats. The interconnected nature of the Internet of Things (IoT) and the widespread adoption of cloud-based computing make them prime targets for future cyberattacks. Nigeria's promising future hinges on large and small organizations' ability to take a proactive stance against cybercrime. Unchecked cyberattacks can lead to devastating consequences, including critical data loss, operational disruptions, and significant financial losses. Cybersecurity safeguards essential systems of information by ensuring three fundamental principles: confidentiality (data is only accessible to authorized users), integrity (systems function as designed), and availability (systems are operational when needed). (Ofori et al., 2017, citing NACCHO, 2015; Securex West Africa, 2017)

Challenges of Cyber Security

The Internet has become essential to our lives, powering everything from banking and communication to education. However, this reliance creates a double-edged sword. As cybercriminals become more skilled, the vast amount of information we store online

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13740477

becomes increasingly susceptible to attack (Ofori et al., 2017). Across Africa, cyberspace is plagued by many security threats, including risks to personal data, intellectual property breaches, and attacks on both domestic and international individuals. Nigeria, unfortunately, is no stranger to these challenges, as cybercriminals target victims both within and beyond its borders. The fight against cybercrime is a relentless race. New threats emerge faster than we can fully comprehend them. Therefore, a comprehensive approach is crucial to address the following cybersecurity challenges:

The digital age, while offering immense opportunities, has introduced complex cybersecurity challenges, particularly in Africa where nations like Nigeria struggle to combat a growing threat landscape (Bada et al, 2019). A significant factor contributing to this vulnerability is the widespread lack of cybersecurity awareness among key stakeholders, including regulators, IT professionals, law enforcement, and the general public (Kshetri, 2019; Turianskyi, 2022). Furthermore, insufficient security measures leave critical systems vulnerable to attack. Nations may struggle to implement or afford robust cybersecurity solutions, making it difficult to defend against sophisticated threats ((Moktar & Rohaizat, 2024).

The absence of solid cybersecurity legislation creates a haven for cybercriminals. Without clear laws and enforcement mechanisms, holding perpetrators accountable or discouraging future attacks is brutal. Additionally, the lack of a well-developed information society can exacerbate these problems. An information society that prioritizes user rights and equal access to data can foster a more secure online environment (Moktar & Rohaizat, 2024).

Finally, a critical shortage of technical expertise further weakens Africa's cybersecurity defences. Nations may lack the skilled personnel to monitor and secure their national systems. This leaves them susceptible to cyber espionage and cyberterrorism activities. Addressing these challenges will be critical for ensuring a safe and secure digital future for Nigeria and other African nations as cyber threats evolve. While national security is a significant concern, cybersecurity issues encompass a broader range of threats (Fard &Verna, 2024).

Theoretical Framework

This study employs crime opportunity theory to appraise Cybercrime and Cybersecurity in the Era of E-Government: Interrogating the Nigerian State; the theory posits that crime is primarily motivated by the availability of opportunities rather than by human biases. Felson and Clarke (1998) contend that opportunities characterized by location, time, target, direction, and manner substantially impact the occurrence of crimes. This theory emphasizes that no crime can arise without some opportunity, highlighting the role of situational circumstances in crime dynamics. As a result, the study's focus on cybercrime within Nigeria's e-government framework is consistent with this theoretical perspective, emphasizing how technological developments and the expansion of digital platforms provide new opportunities for cybercriminals.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13740477

The study contributes to scientific knowledge in Nigeria by exploring how the proliferation of e-government services and digital tools has facilitated and exacerbated cybercrime. The theory's assertion that reducing criminal opportunities is essential for crime prevention is particularly relevant. The study provides actionable insights into mitigating these opportunities by investigating how specific technological and situational factors within Nigeria's e-government systems can be targeted to minimize cybercrime. It challenges existing notions of cybercrime by illustrating those technological advancements, while beneficial, can inadvertently create new avenues for criminal activity.

Moreover, the study's application of the crime opportunity theory to the Nigerian context offers an understanding of how e-government innovations intersect with cybersecurity challenges. It demonstrates that, while technological progress is inevitable, it is crucial to proactively address the emerging opportunities for cybercrime that come with it. This contribution is significant as it not only enhances theoretical understanding but also informs practical strategies for cybersecurity, advocating for a balance between embracing technological advancements and implementing effective crime prevention measures.

METHODOLOGY

This research adopts a quantitative approach, utilizing a survey design to gather primary data through a structured questionnaire. The data collection process involved simple random selecting responses from preselected Ministries, Departments, and Agencies (MDAs) that have fully integrated e-government services into their operations. These include the Kaduna State Budget and Planning (KADBP), Kaduna State Geographic Information Service (KADGIS), Kaduna State Internal Revenue Service (KDIRS), and Kaduna State Urban Planning and Development Authority (KASUPDA).

The study's target population consists of 1,190 government employees distributed among these MDAs: KADBP (209 employees), KADGIS (262 employees), KDIRS (469 employees), and KASUPDA (250 employees). From this population using the Taron Yamane, a sample of 381 respondents who actively utilize e-government services was randomly selected for the study. The structured questionnaire was meticulously designed to capture a range of measures that could be implemented to mitigate the effects and prevalence of cybercrimes. Data analysis used Multiple Regression with the Statistical Package for the Social Sciences (SPSS) version 26.0 to interpret the collected data and derive meaningful insights.

Data analysis and Discussions

The data collected through the structured questionnaire from the sampled organizations under study were analyzed descriptively using frequencies and simple percentages. In contrast, the hypothesized variables were analyzed using Multiple Regression via the Statistical Package for the Social Sciences (SPSS) Version 26.0. The responses on the questionnaire are rated on a 5-point scale, with all positive statements ranging from 5-1

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13740477

for different response categories. Strongly agree (SA), Agree (A), Undecided (U), Disagree (DA) and Strongly Disagree (SDA). Hence, expert opinions on the variables were sought from knowledgeable and experienced employees in e-government-enabled organizations and cyber experts. All corrections and modifications were made were affected accordingly to adequately capture the objective of the study. A total of 400 copies of the questionnaire were circulated and 381 were returned and measured, in other words, a response rate of 95.25% was achieved. This is considered adequate for further analysis.

Descriptive Analysis

Tables, frequencies, and simple percentages were used to analyze the causes and effects of cybercrime in Nigeria, particularly regarding MDAs in Kaduna State.

Table 1: Causes of Cybercrimes in Nigeria

Causes	Frequency
Poverty	129
Unemployment	80
Substandard educational system	12
Austere financial conditions	19
Quest for affluence	57
Internet addiction	8
Vulnerable cybersecurity	31
Corruption	45
Total	**381**

Source: Field Survey, 2024

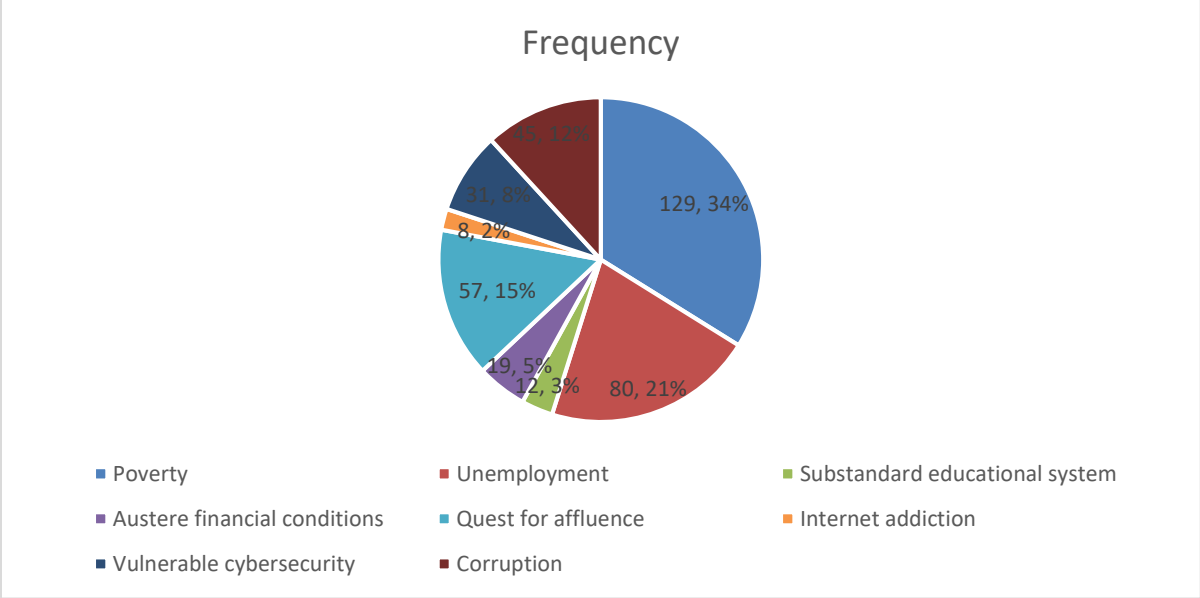

Figure 1: Causes of Cybercrimes in Nigeria

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13740477

Figure 1 shows that out of 381 respondents, 129, representing 34%, indicated that poverty is Nigeria's primary cause of cybercrimes. Poverty, generally speaking, is one of the primary and significant push factors propelling people to seek quick financial gains to cater to their needs and those of their families and loved ones.

It was also revealed that 80 respondents, representing 21%, indicated that unemployment is another significant cause of cybercrime in Nigeria. Research has shown that unemployment is another essential push factor compelling Nigerians, particularly the youth, to engage in cybercriminal activities with the hope of enjoying quick financial gains out of the wealth of others.

Similarly, 12 respondents, representing 3%, indicated that the country's substandard educational system is another significant cause of cybercrime. Over the years, a lack of sufficient education and awareness about cybersecurity risks and digital ethics has contributed significantly to cybercriminal activities in Nigeria. Many cyber criminals in Nigeria and around the world usually host the elderly and vulnerable with the hope of taking advantage of their lack of adequate knowledge of cybersecurity.

Similarly, 19 respondents, representing 5%, indicated that austere financial conditions are a salient and significant cause of cybercrime in Nigeria. This implies that many cybercriminals usually engage in cybercrime due to their poor economic conditions, hoping to scam people, particularly the rich, of their money and other financial resources. It is also important to note that some other cybercriminals usually engage in cybercriminal activities due to greed and lack of contentment with their present economic conditions.

Complementing this, 57 respondents, representing 15%, indicated that the quest for affluence is a significant cause of cybercrime in the country. The pursuit of affluence, particularly by the present young generation, is alarming; many youths these days engage in cybercriminal activities due to social influence and the quest for easy money to impress ladies and their friends. The influence of the social circle of the youths today, as well as their pursuit of easy and quick affluence to impress and suppress others, is becoming unbearable due to the large number of yahoo-boys in the country.

Among some of the critical causes of cybercrime in Nigeria is internet addiction. Research has shown that 8 respondents, representing 2%, indicated that internet addiction is also one of the major causes of cybercrime in the country. The rate of cybercrime in Nigeria is gradually unbecoming due to the development of ICT, the Internet, and social media, thereby exposing the people, particularly the youth, to a whole new platform where cybercriminal activities can be perpetrated to the detriment of the victims.

In agreement, 31 respondents, representing 8%, indicated that vulnerable cybersecurity is another salient cause of cybercrime in the country. Many people today engage in cybercriminal activities due to Nigeria's high level of cybersecurity vulnerability. The presence of ineffective cyber laws and enforcement and the lack of sufficient resources for effective cybersecurity are significant factors for cybercrime in Nigeria. Corroborating the above, 45 respondents, representing 12%, indicated that corruption is one of the considerable causes of cybercrime in Nigeria. The high level of corruption in Nigeria,

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13740477

particularly in the public sector, has created a room whereby cybercrimes are tolerated and overlooked. This has further allowed other individuals to also engage in cybercriminal activities. Addressing these causes requires a multi-faceted approach involving education, more robust legal frameworks, and enhanced law enforcement capabilities.

Table 2: Effects of cybercrime

Effects	Frequency
Low productivity	58
Service disruption	61
Loss of confidence resulting from leakage of confidential data	49
Loss of revenue	76
Damage to national image	137
Total	**381**

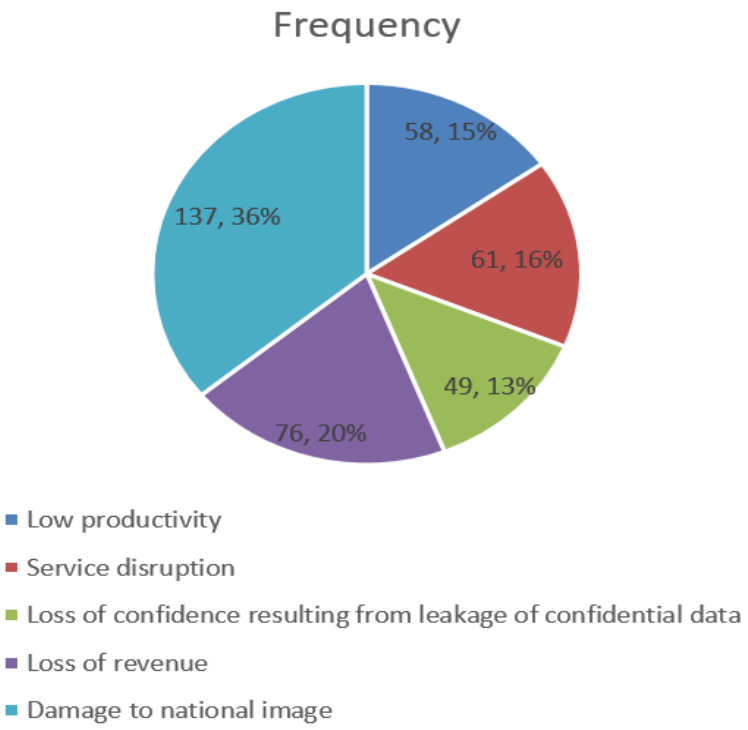

Figure 2: Effects of cybercrime

Figure 2 shows that out of 381 respondents, 137 respondents, representing 36%, indicated that one of the significant effects of cybercrime in Nigeria is damage to the national image. Labelling Nigeria as one of the countries with the highest number of cybercriminals is one of the significant adverse effects of cybercrime, which tarnishes its national image and reputation, affecting its tourism, foreign investment, and business partnerships, among others. This implies that due to the high level of cybercrime in Nigeria, many foreign investors see Nigeria as an unattractive market for future

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13740477

businesses. As a result of this, Nigeria is listed as one of the most corrupt countries in the world (Igba, Igba, Nwambam, Egbe, & Ogodo, 2018).

Similarly, 58 respondents, representing 15%, indicated that **low productivity** in public service delivery is another significant negative effect of cybercrime in Nigeria. Due to service interruptions, many Ministries, departments, and agencies are performing below standard. Due to measures such as shutting down servers, many MDAs usually experience poor productivity. According to Igba, Igba, Nwambam, Egbe, and Ogodo (2018), many private companies, particularly those in developing countries, usually block email traffic from Nigeria for fear of cyber criminals. Also, some international banks have ultimately denied Nigerians access to their website if the traffic originates from Nigeria.

In the same way, 76 respondents, representing 20%, indicated **financial loss or loss of revenue**. To individuals and organizations, cybercriminals usually target individuals and organizations from which they can make significant economic gains. To an economy, one of the main adverse effects of cybercrime is loss of revenue. To financial institutions or multinational corporations, loss of income can be caused by an outside party who obtains sensitive financial information and uses it to withdraw funds from the account of such an institution. Cybercriminals usually hack an organization or MDAs' e-commerce site while the site has been compromised and inoperable; valuable revenue is lost when consumers are unable to use the site (Igba, Igba, Nwambam, Egbe, & Ogodo, 2018).

Corroborating this, 49 respondents, representing 13%, indicated a **loss of confidence** in the system resulting from confidential data leakage. In comparison, the remaining 61 respondents, representing 16%, stated service interruption is a significant effect of cybercrime in Nigeria. According to Igba, Igba, Nwambam, Egbe, and Ogodo (2018), many individuals, organizations and countries usually lose confidence in dealing with the government when cybercriminals have intercepted their credit card or other financial data; as such, they prefer to do business dealings with other countries or organizations.

Multiple Regression Analysis

Multiple Regressions were used to determine the various effects of capacity building, enhanced funding and resources, established incidence response and recovery plan, modernization of IT systems, and public awareness campaigns on cyber security in Kaduna State. The preliminary analysis of the multiple regression is discussed below:

Table 3: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.765[a]	.586	.580	.35313

a. Predictors: (Constant), Public Awareness Campaigns, Established Incidence Response and Recovery Plans, Capacity Building, Enhanced Funding and Resources, Modernization of IT System

Source: Authors (2024)

Table 3 above shows the summary of the Multiple Regression analysis. The empirical findings show that R, the multiple correlation coefficient, stood at 0.765, which indicates a high correlation between capacity building, enhanced funding and resources,

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13740477

established incidence response and recovery plan, modernization of IT systems, public awareness campaigns and cyber security in Kaduna State. R^2, the multiple coefficients of determination of the variables stood at 0.586, indicating that about 58.6% of the total variation in cyber security in Kaduna State is explained by variations in the independent variables (capacity building, enhanced funding and resources, established incidence response, and recovery plan, modernization of IT systems, and public awareness campaigns) captured in the study. The adjusted $R^{2,}$ being 0.580, also indicates that the independent variables will still explain 58% of the variations in cyber security in Kaduna State, even if other variables were added to the study.

Table 4: Analysis of Variance (ANOVA[a])

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	66.062	5	13.212	105.951	.000[b]
	Residual	46.763	375	.125		
	Total	112.825	380			
a. Dependent Variable: Cyber Security						
b. Predictors: (Constant), Public Awareness Campaigns, Established Incidence Response and Recovery Plans, Capacity Building, Enhanced Funding and Resources, Modernization of IT System						

Source: Authors (2024)

In Table 4, the results from the multiple regression analysis, which tests the effects of the independent variables (capacity building, enhanced funding and resources, established incidence response and recovery plan, modernization of IT systems, and public awareness campaigns) on the dependent Variable, cyber security in Kaduna State is shown. The F-statistic, which measures the adequacy and fitness of the model used in the study, stood at 105.212 with a p-value of $0.000^{b,}$ which is significant at 5%; this shows that the model is fit for the study.

Table 5: *Correlation Coefficient (Coefficients[a])*

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.542	.172		3.151	.002
	Capacity Building	.105	.036	.124	2.900	.004
	Enhanced Funding and Resources	.225	.037	.256	6.117	.000
	Established Incidence Response and Recovery Plans	.007	.021	.012	.342	.733
	Modernisation of I.T. System	.199	.045	.208	4.383	.000
	Public Awareness Campaigns	.386	.046	.366	8.385	.000
a. Dependent Variable: Cyber Security						

Source: Authors (2024)

Table 5 shows the outcome of the respective independent variables (capacity building, enhanced funding and resources, established incidence response and recovery plan, modernization of IT systems, and public awareness campaigns) on cyber security in Kaduna State. These are further discussed under the test of hypotheses section.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13740477

Hypotheses Testing

Multiple regression was used to test the numerous relationships between the study's independent and dependent variables. The hypotheses were tested using Statistical Package for the Social Sciences (SPSS) version 26.0.

Hypothesis I - VI

Ho_1: There is no significant relationship between capacity building and cyber security in Kaduna State

Ho_2: There is no significant relationship between enhanced funding and resources and cyber security in Kaduna State

Ho_3: There is no significant relationship between established incidence response and recovery plan and cyber security in Kaduna State

Ho_4: There is no significant relationship between the modernization of IT systems building and cyber security in Kaduna State

Ho_5: There is no significant relationship between public awareness campaigns and cyber security in Kaduna State

The coefficients of capacity building enhanced funding and resources, established incidence response and recovery plan, modernization of IT systems, and public awareness campaigns stood at 0.105, 0.225, 0.007, 0.199, 0.386, which is positive with a p-value of 0.004; 0.000; 0.733; 0.000, and 0.000. The p-values are less than 5%, except for established incidence response and recovery plans; this implies that an increase in capacity building, enhanced funding and resources, established incidence response and recovery plan, modernization of IT systems, and public awareness campaigns in Kaduna State would lead to a corresponding increase of 10.5%; 22.5%; .7%; 19.9% and 38.6% respectively on cyber security in Kaduna State. However, its significance can be judged from the statistics.

The t statistics of capacity building enhanced funding and resources, established incidence response and recovery plan, modernization of IT systems, and public awareness campaigns stood at 2.900, 6.117, 0.342, 4.383, and 8.385, respectively, with a p-value of 0.004; 0.000; 0.733; and 0.000 respectively. The p-values are less than 0.05, except for established incidence response and recovery plans, indicating that the relationship depicted in the model is significant at a 95% confidence level. This implies that the study lacks statistical evidence to accept all the null hypotheses.

Based on the above analyses, the study fails to accept the null hypotheses **HO_{1-4},** which state that there is no significant relationship between capacity building, enhanced funding and resources, established incidence response and recovery plan, modernization of IT systems, public awareness campaigns and cyber security in Kaduna State; and accept their alternate hypotheses. In other words, all the independent variables (i.e., capacity building, enhanced funding and resources, modernization of IT systems, and public awareness campaigns) depict a positive and significant relationship with cyber security in

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13740477

Kaduna State except for the established incidence response and recovery plan. By adopting these measures, Nigeria, particularly Kaduna State, can enhance the cybersecurity posture of its e-government initiatives, safeguard sensitive data, maintain public trust, and effectively mitigate the evolving cyber threats facing digital governance in the State.

CONCLUSION

This paper demonstrates that the borderless nature of crime makes transnational crime a significant security concern in today's international relations, with cybercrime exemplifying this perfectly. A cyberattack originating in one country can ripple across borders, impacting other nations and compromising critical systems. The Internet, which underpins many essential services, makes cyberattacks a significant threat to national and economic security. These online assaults endanger sensitive information and infrastructure, potentially weakening a nation's economy. Also, the ever-evolving technological landscape creates a double-edged sword; while it brings advancements, it also presents ongoing threats in cyberspace. The rise of cybercrime can have devastating consequences for individuals, organizations, and entire nations. Therefore, internet users must be increasingly aware of these threats and take steps to protect themselves. Although eliminating cybercrime may be unrealistic, specific measures can be taken to prevent its occurrence or mitigate its effects. Plugging the security gaps that cybercriminals exploit can make it much harder for them to succeed. Cybercrime threatens Nigeria's economy, reputation, productivity, and critical information infrastructure, making robust cybersecurity practices essential.

The study highlights that the data collected reveals a positive and significant relationship between capacity building, enhanced funding and resources, established incidence response and recovery plans, modernization of IT systems, public awareness campaigns, and cybersecurity in Kaduna State. While the relationship between incidence response and recovery plans and cybersecurity was positive but insignificant, the analysis showed that increasing capacity building, funding, modernization of IT systems, and public awareness campaigns led to a significant positive increase in cybersecurity. Based on these findings, the study recommends that the Kaduna State government ensure continuous staff training on identifying and mitigating cyberattacks, recruiting skilled personnel, and fostering collaboration between government and cybersecurity experts. Imposing strict sanctions on cybercriminals is also crucial to deter them from engaging in such activities.

Additionally, the study suggests that the government should invest in cybersecurity infrastructure and allocate budgets to cybersecurity initiatives and collaborations. Implementing swift and updated incidence response and recovery plans can mitigate the effects of cybercrimes. Periodic cybersecurity assessments and audits should be conducted to identify and address vulnerabilities, and emergency response measures such as shutting down primary servers should be designed for proper implementation. The study also recommends implementing biometric verification systems to prevent

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13740477

unauthorized access, using sophisticated online monitoring and surveillance tools to detect hacking attempts, employing blockchain technology for secure credentialing, and using data encryption to render stolen data unusable. Public awareness campaigns through various media should educate the public on identifying cyberattacks and practising safe online habits. Educating the public on protecting their information from cybercriminals is essential in fostering a secure cyberspace.

References

1) Agbozo, E. (2018). The role of data-driven e-government in realizing the sustainable development goals in developing economies. *Journal of Information Systems & Operations Management, 12*(1), 70–77.

2) Anichebe, A. (2019). Effect of integrated personal payroll information system on employee welfare: Evidence from federal ministries in Nigeria. *Australian. Journal of Arts and Scientific Research*, *22*(1), 1–143. Retrieved from https://www.researchgate.net/publication/333816775

3) Al-Amro, S. (2016). Cybercrime and its impact on the Middle East's e-government services and the private sector. *International Journal of Computer Science and Information Security, 14*(3), 69.

4) Alese, B. K., Thopson, O.F., Owa, K. V., Iyare, O & Adebayo, O. T. (2014). Analyzing issues of cyber threats in Nigeria. *Proceedings of the World Congress on Engineering, 1*, 1-6. London: UK.

5) Bada, M., Von Solms, B., & Agrafiotis, I. (2019). Reviewing national cybersecurity awareness in Africa: An empirical study.

6) Button M., Shepherd D., Blackburn D., Sugiura L., Kapend R., and Wang V. (2022). Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective. *Criminology & Criminal Justice*, 1-22. https://doi.org/10.1177/17488958221128128

7) Cerrudo, C. (2017, January 17th). Why cybersecurity should be the biggest concern of 2017. Forbes community voice. Retrieved March 20th, 2024 from. https://www.forbes.com /sites/forbestechxouncil/2017/01/17/why cybersecurity-should –be the biggest concern 2017d

8) Chigozie- C.C., Micheal, D.O. & Ugboaja, S.G (2017). Computer forensics investigation: implications for improved cybersecurity in Nigeria. *International Journal of Science and Technology 6*(1), 59-73.

9) Chung, M., & Kim, J. (2019). The Internet information and technology research directions are based on the fourth industrial revolution. *KSII Transactions on Internet and Information Systems*, *10*(3), 1311–1320.

10) Cole, K., Chetty, M., LaRosa, C., Rietta, F., Schmitt, D. K., Goodman, S. E., & Atlanta, G. A. (2008). Cybersecurity in africa: An assessment. *Atlanta, Georgia, Sam Nunn School of International Affairs, Georgia Institute of Technology*.

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

12) Dasuki, M. S. (2014). National cybersecurity policy. Retrieved March 20th, 2018.

13) Eggers, W. D. (2016, July 25th). Cyber challenge: Protecting sensitive data for the public good. *Deloitte Review*, 19. Retrieved March 20th, 2024 from https://www2,deloitte.com/insight/us/en/deloitte-review/issue-19/protecting sensitive data-government-cybersecurity.html

14) Fard, AE and Verma T, A comprehensive review on countering in the age of online social media platforms. In Causes and symptoms of socio-cultural polarisation: Role of information and communication technology; Springer: Berlin/Heidelberg, Germany, 2022; pp. 253-284 (Google Scholar)

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13740477

15) Fisher, E.A. (2016). Cyber security issues and challenges: In Brief. *Congregational Research Service Report (Report no. R43831).* Retrieved March 20th, 2024 from*: www.crs.gov*

16) Gberevbie, D.E., Ayo, C. K. Iyoha, F. O. Duruji, M. M. & Abasilim, U.D. (2018). Electronic governance platform: towards overcoming the challenges of non-inclusion of citizens in Nigeria's public policy formulation and implementation. *International Journal of Electronic Governance, 10*(1), 56–73, 2018

17) Giles, M. (2018). Six cyber threats to worry about in 2018. Retrieved March 20th, 2018 From: https://www.technologyreview .com/609641/six-cyber-threats-to-really-worry-about-in-2018

18) Heikkila, A. O (2018). Cyber security trends and threats to watch for in 2018. Retrieved March 20th, 2018, from https:/ https://harckernoon.com/cuber-security-trends-and-threats-to-watch-for-in- 2018-a13cOf843d65

19) Ibikunle, F. & Eweniyi, O (2018). Approach to cyber security issues in Nigeria: Challenges and solutions. *International Journal of Cognitive Research in Science, Engineering Education, 1*(1), 100–110.

20) Kshetri, N. (2013). *Cybercrime and cybersecurity in the global south*. UK: England. Palgrave Macmillan

21) Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77-81.

22) Lubis M. and Handayani D. O. D. (2022). The relationship of personal data protection towards internet addiction: Cybercrimes, pornography and reduced physical activity, *Procedia Computer Science*,.179, 151-161. https://doi.org/10.1016/j.procs.2021.12.129

23) Maad, M.. & Muhammad, A. (2023). Towards Artificial-Based Cybersecurity: The practice and CharGPT Generated ways to combat cybercrime. https://journal.esj.edu.iq/index.php/IJCm.

24) Makeri, Y. A. (2017). Cybersecurity issues in Nigeria and challenges. *International Journal of Advanced Research in Computer Science and Software Engineering. 7*(4), 315–321. A publication of Kampala International University

25) Michael, J. & Deepamalar, M. (2017). Anti-cybercrime technologies for e-governance," *International Journal of Innovative Research in Science, 6*(5), 7957–7963

26) Miller, J. M., Higgins, G. E. & Lopez, K. M. (2013). Considering the role of e-government in cybercrime awareness and prevention: Toward a theoretical research program for the 21st century, In Digital Rights Management: Concepts, Methodologies, Tools, and Applications. *IGI Global*, 789–800.

27) Mokhtar, R., Rohaizat, A. (2024). Cybercrimes and Cyber Security Trends in the New Normal. In: Kamaruddin, N., Idries, A., Fernandez, K. (eds) The New Normal and its Impact on Society. Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-97-0527-6_4

28) Odumesi, J.O. (2014). Combating the menace of cybercrime. *International Journal of Computer Science and Mobile Computing, 36*, 980–991.

29) Offorgi, J.C. Udensi, E. J. &Ibegbu, K.C (2019). Cybersecurity challenges in Nigeria: The way forward. *Journal of Cyber Criminology, 9*(1), 120-143.

30) Oni, S., Berepubo, K.A., Oni, A.A. & Joshua, S. (2024). *E-government and the challenge of cybercrime in Nigeria*. Unpublished Journal, Department of Political Science and International Relations Covenant University Nigeria.

31) Premiums Times Nigeria. (2017, August). Nigeria ranks 3rd in global internet crimes behind the UK, US-NCC. Retrieved March 20th, 2018 From https://www.premiumtimessng.com/news/top-news/top-news241160-nigeria-rqnks-3rd-global-internet-crime-behind UK-S-Sncc.html

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13740477

32) Saini, West Africa. (2017, November 16th). Cyber Security in Nigeria Needs to be a Priority and Here's Why. Retrieved March 20th, 2018, From https://www.securexwesafrica.com/news-desk/deteil/cyber-security-in-nigeria-needs-to-be-a-priority-and-heres-why

33) Sean, D., (2023) lead Cyber Initiative, world economic summit

34) Tabansky, L. (2012). Cybercrime: A national security issue? *Military and Strategic Affairs, 4*(3), 117-136.

35) Tao, F., Akhtar, M. S., & Jiayuan Z. (2021). The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, *EAI Endorsed Transactions on Creative Technologies*, *8*(28), 1-15. https://doi.org/10.4108/eai.7-7-2021.170285

36) Turianskyi, Y. (2022). *Balancing cyber security and internet freedom in africa*. South African Institute of International Affairs.

37) Vashik, C., Matsubara, M. & Plonk, A. (2016). Key concepts in cyber security: Towards a standard policy and technology context for cyber security norms". In Osula, A & Roigas, H (Eds.), I*nternational cyber norms: Legal Policy & Industrial Perspective* 221-2420.Tallinn, Estonia: NATO CCD COE publication

38) V. R. Gajjar and H. Taherdoost, "Cybercrime on a Global Scale: Trends, Policies, and Cybersecurity Strategies," *2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)*, Lalitpur, Nepal, 2024, pp. 668-676, doi: 10.1109/ICMCSI61536.2024.00105.