AN EXAMINATION OF CYBERSECURITY AND CYBERCRIME LAWS IN NIGERIA

Ibhade Oluwabunlola Adisa-Ibojo[*], Olayinka David Afolabi[**], Nasirudeen Ade Muslim[***]& Wilson Sakpere[****]

Abstract

Cybercrime has become a thorn in the flesh of individuals and society leading to challenges like malware, phishing, and cyber bullying seemingly overshadowing the benefits of the cyberspace. This paper peruses cyber-security and cybercrime as a dimension of cyber threat in the biosphere. It goes further to examine the perpetrators of cybercrime; introduces the concept of cyber-security on another plane and the types of cyber-security. This paper aims to explore cyber-security and cybercrime law as variety of threats for which Cybersecurity antagonizes the benefits of Cybersecurity, and the underlining principles of Cybersecurity. It examines the existing statutory provisions which are available to the Nigerian legal system; with a view at the liability-extent of offenders of these laws. This is a qualitative research that employs doctrinal method of study through the use of primary and secondary sources of information. The paper finds that improvement in technology has paved way for cyber-

[*] LL.B (Hons.), BL, LL.M, PhD candidate and Lecturer, Department of Private and Business Law, Lead City University, Ibadan.

[**] LL.B (Hons.) BL, LL.M, PhD candidate at Lead City University, Judge of Osun State High court, Osun state.

[***] LL.B (hons), BL, LL.M, PhD candidate at Lead City University, Lecturer, General Studies Department, OkeOgun polytechnic, Saki, Oyo State

[****] BEng (Electrical), MTech (information Technology), PhD (Computer Science and Engineering) Lecturer, Department of Computer-Science, Lead City University, sakpere.wilson@lcu.edu.ng

crimes, there is thus need for government to rise to the occasion of implementing the laws to curb the menace of cyber-crime.

Keywords: Criminal law, criminal liability, cybercrime, cyber-security, cyberspace.

1.0 Introduction

Cybersecurity is the defense against harmful assaults by hackers, spammers, and cybercriminals against internet-connected devices and services.[1] Businesses utilize this procedure to safeguard themselves from phishing scams, ransomware attacks, identity theft, data breaches, and financial losses.[2] Today's world is more dependent on technology than ever before, as you can tell by looking around. The advantages of this trend include nearly instantaneous information availability via the Internet and contemporary comforts offered by technologies like smart home automation and the Internet of Things.[3]

It might be difficult to accept that potential risks hide behind every gadget and platform when technology has brought us so much good. Cybercrime is any criminal activity that utilizes computers and the Internet.[4] Despite how positively society views technological advancements, there is still a serious risk from modern technology's cyber security dangers.[5]

[1]Christina Meileewilliams and others, 'Cybersecurity Risks in a Pandemic' [2020] 22(9) Journal of Medical Internet Research 200.

[2]Ricardo Jorge raimundo and AlbéricoTravassosRosário, 'Cybersecurity in the Internet of Things in Industrial Management' [2022] 12(3) Applied Sciences 1598.

[3]Makoiedova V, 'Information Technology: Approaches to Definition, Principles of Construction' (2022)2 Cybersecurity: Education, Science, Technique 138.

[4]Ian J Lloyd, Information Technology Law (9th edn, Oxford University Press 2020)7.

[5] ibid.

Cybercrime can be perpetrated against a person, a group of people, as well as public and private organizations.[6] It might be done to cause someone bodily, mental, or reputational harm.[7] Depending on whom the victim is, cybercrime may affect them directly or indirectly.[8]It's critical to be aware of potential hazards in our online space, as these dangers are unpredictable, lethal, and cunning.[9] The protection we offer for our personal and corporate data should be the same. By safeguarding our company's data, preventing financial loss, ensuring business continuity, and maintaining your reputation, cyber security will be advantageous to us.[10]

Because we now rely on the internet for both our everyday business and social contacts, cyber security and cybercrime are two interrelated phenomena that are here to stay.[11]However, both personal and governmental financial security is under the greatest threat from cybercrime.[12] The vulnerabilities in the gadgets and services we've grown to rely on are highlighted by the constant growth in cybercrime. Because of this worry, we must consider what cyber security is, why it's important, and what we can learn about it.[13] In the media, the phrase "cyber security" has become a catch-all for the process of preventing any type of cybercrime, from identity theft to the deployment of international

[6]Syamsuddinishak and others, 'Analysis of Imprisonment Implementation against the Perpetrators of the Cybercrimes' [2023] 4(2) Journal of Social Sciences 320-337.
[7] ibid.
[8]Nwafor I E,*Cybercrime and the law: Issues and developments in Nigeria* (Kraft Books Limited 2022).
[9] ibid.
[10]HatemAbdulkader, 'Protecting Online Social Networks Profiles by Hiding Sensitive Data Attributes' [2016] 82(4) Elsevier 20-27.
[11]ZarynDentzel, Tuenti, Dentzel Z and Tuenti, 'How the Internet Has Changed Everyday Life'(*OpenMind*) <https://www.bbvaopenmind.com/en/articles/internet-changed-everyday-life/> accessed 22 October 2023.
[12]Joe Kim, 'Cyber-security in government: reducing the risk' [2017] 17(7) Elsevier 8-11.
[13] ibid.

digital weapons.[14] These classifications are accurate, but they fall short of describing the full nature of cyber security for persons without a background in computer science or the digital sector.[15]
Cybersecurity is defined as "...the practice of protecting systems, networks, and programs from digital attacks" by Cisco Systems, a tech giant that specializes in networking, the cloud, and security. These hacks often try to disrupt regular corporate operations, extort money from users, or access, alter, or delete important information.[16]

2.0. Cybersecurity

Cyber security refers to the technology, techniques, and strategies used to protect computer systems, data, and networks against cyber threats. To effectively answer the topic "what is cyber security" and how it works, we must break it into many subdomains[17]

2.1. Types of Cyber Security

a. **Application security** is the application of various defenses in an organization's software and services to protect against a wide variety of threats. To reduce the possibility of illegal access or alteration of application resources, cyber security specialists must develop safe code, build secure application architectures, implement strong data input validation, and perform other tasks.[18]
b. **Cloud security** is concerned with developing safe cloud infrastructures and applications for businesses that employ cloud

[14] ibid.
[15] ibid.
[16] Jonathan Lewallen, 'Emerging technologies and problem definition uncertainty: The case of cybersecurity' [2021] 15(4) Regulation and Governance 1035-1052.
[17] Thakur K and Pathan A-SK, 'Types of Cyberattacks' [2020] Cybersecurity Fundamentals 41.
[18] ibid.

service providers such as Amazon Web Services, Google, Azure, Rackspace, and others[19].

c. **Data Security and Identity Management** subdomain includes actions, structures, and processes that enable lawful persons to access an organization's information systems. These procedures entail putting in place sophisticated information storage methods that safeguard data while it is in transit or on a server or device. Furthermore, this sub-domain employs more authentication techniques, whether two-factor or multi-factor.[20]
d. **Mobile Safety** safeguards organizational and personal data held on mobile devices such as tablets, cell phones, and laptops against various dangers like as illegal access, device loss or theft, malware, viruses, and so on. Furthermore, mobile security incorporates authentication and education to aid increase security.[21]
e. **Network Safety** refers to the hardware and software methods that safeguard the network and infrastructure from outages, illegal access, and other abuses. Effective network security safeguards organizational assets against a wide range of dangers, both internal and external to the business.[22]
f. **Business Continuity and Disaster Recovery Planning** is another type. Not all hazards are caused by humans. The DRBC subdomain includes processes, alerts, monitoring, and plans to assist organizations in preparing to keep their business-critical systems operational during and after any type of incident (massive power outages, fires, natural disasters), as well as

[19]ibid.
[20] A. Bhardwaj and V. Kumar, 'Cloud security assessment and identity management', 14th International Conference on Computer and Information Technology (ICCIT 2011), p. 387-392, doi: 10.1109/ICCITechn.2011.6164819.
[21]John Sammons and Michael Cross, The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy (2nd edn, Syngress 2017) 18.
[22] ibid.(P 14).

resuming and recovering lost operations and systems in the aftermath of the incident[23].

2.2. Cybersecurity Environment

The cyber threat landscape describes the ever-changing nature of cyber threats, which can range from malware and phishing assaults to ransomware and data breaches.[24] These risks may originate from a range of sources, including nation-state actors, organized criminal syndicates, and individual hackers.[25]

The fast speed of technological development is one of the most difficult issues in controlling the cyber threat scenario. As new technologies are created and deployed, they may provide new vulnerabilities that attackers might exploit. For example, the expansion of the Internet of Things (IOT) has resulted in a large network of linked devices that hackers may exploit[26].

The rising sophistication of cyber assaults is another issue in controlling the cyber security scenario. Cybercriminals are continually devising new methods to circumvent security measures and avoid discovery, making it increasingly difficult for businesses to safeguard themselves.[27]

By having a strong Cybersecurity plan, businesses can remain ahead of the cyber threat scenario. Technical protections, like as firewalls and intrusion prevention systems, should be included, as should non-

[23]Susan snedaker and Michael Cross, Business Continuity and Disaster Recovery Planning for IT Professionals (2nd edn, Syngress 2014) 3

[24]Nektariakaloudi and Jingyue li, 'The AI-Based Cyber Threat Landscape: A Survey' [2020] 53(1) ACM Journals 1-34.

[25] ibid.

[26]Niell C and others, 'BCG's Annual Cybersecurity Survey 2023: As Budgets Get Tighter, Cybersecurity Must Get Smarter' (*BCG Global*, 4 September2023)<https://www.bcg.com/publications/2023/navigating-the-new-cybersecurity-environment> accessed 22 October 2023.

[27]Kushagra pal and others, 'Implementation of Artificial Intelligence Methods to Curb Cyber Assaults: A Review' [2018] 5(9) International Research Journal of Engineering and Technology 1-4.

technical measures, such as staff awareness training and incident response plans.[28]

Overall, controlling the cyber threat landscape necessitates a continual and proactive strategy. Organizations may better protect themselves against cyber-attacks and lower the likelihood of a successful breach by staying up to date on the newest threats and employing appropriate security measures.[29]

The cyber threat landscape is significant for several reasons. To begin, companies must understand the many sorts of cyber dangers that they may encounter in order to appropriately protect themselves against these attacks. Understanding the methods, techniques, and processes utilized by attackers, as well as the motives behind these attempts, is part of this.[30]

Another argument for the importance of the cyber threat landscape is that it may assist firms in prioritizing their cyber security activities. They may focus their resources by assessing the most serious dangers to their organization[31].

Understanding the cyber threat environment may help firms respond more effectively to events that do occur, in addition to helping them protect themselves against cyber-attacks.[32] They can more rapidly identify the source of an attack and conduct suitable countermeasures if they have a thorough awareness of the many sorts of risks that face their business.[33]

Finally, the cyber threat environment is crucial because successful cyber-attacks may have serious ramifications for enterprises. This can

[28] ibid.
[29] ibid.
[30]Kim Kwangraymondchoo, 'The cyber threat landscape: Challenges and future research directions' [2011] 30(8) Elsevier 719-73.
[31]ibid.
[32]Nektariakaloudi and others, 'The AI-Based Cyber Threat Landscape: A Survey' [2020] 53(1) Association for Computing Machinery 1-34.
[33] ibid.

involve financial losses, reputational harm, and legal responsibilities. Organizations may better protect themselves and their stakeholders by knowing the cyber threat landscape and adopting actions to mitigate these dangers.[34]

2.2.1 Current Cyber Threats Environment

The present cyber threat landscape is continually changing, with new threats appearing on a regular basis.[35] Among the most serious dangers confronting businesses today are

a. **Ransomware:** This sort of malware encrypts data and demands a ransom in exchange for the decryption key. Ransomware attacks may cause major financial losses as well as disruption for impacted businesses.[36]
b. **Phishing attacks:** These include attackers sending bogus emails or text messages that look to be from genuine sources in an attempt to fool people into disclosing sensitive information such as login credentials or financial information.[37]
c. **Malware**: Malware is a general word for any program that is intended to harm or disrupt computer systems. This can contain viruses, worms, and Trojans, among other types of malware.[38]
d. **Data breaches**: Data breaches occur when attackers obtain unauthorized access to an organization's data, either by hacking

[34] ibid.
[35]Thomas wagner and others, 'Cyber threat intelligence sharing: Survey and research directions' [2019] 87(1) Computers and security 109.
[36]Savitamohurle and Manishapatil, 'A brief study of Wannacry Threat: Ransomware Attack 2017' [2017] 8(5) International Journal of Advanced Research in Computer Science 1938-1940.
[37] S. Gupta, A. Singhal and A. Kapoor, 'A literature survey on social engineering attacks: Phishing attack', 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India. p. 537-540, doi: 10.1109/CCAA.2016.7813778.
[38]OriOr Meir, 'Dynamic Malware Analysis in the Modern Era; A State of the Art Survey' [2019] 52(5) ACM Journals 1-48.

into the organization's systems or exploiting security flaws. These assaults can result in the loss of sensitive information and have serious ramifications for the companies that are targeted.[39]

e. **Nation-state cyber espionage:** As a way of gathering intelligence and harming the interests of other countries, nation-state actors have increasingly turned to cyber assaults. These assaults may be quite sophisticated, affecting a wide range of institutions, including governments, corporations, and essential infrastructure.[40]
f. **Cyber-terrorism:** This is a politically motivated attack on computers and information technology with the intent of causing harm and broad societal disturbance[41].
g. **Botnets**: This particularly heinous attack entails large-scale cyber-attacks carried out by remotely controlled malware-infected machines. Consider it a network of computers coordinated by a single cybercriminal. Worse, infected machines become part of the botnet system.[42]
h. **Adware:** Adware is a type of malware. It's also known as ad-supported software. Adware is a potentially unwanted program (PUP) that is loaded without your knowledge and creates annoying web adverts.[43]

[39]Long Cheng and others, 'Enterprise data breach: causes, challenges, prevention, and future directions' [2017] 7(5) Wiley interdisciplinary reviews 1-14.
[40]Kosejoab, 'Cyber Warfare: An Era of Nation-State Actors and Global Corporate Espionage' [2021] 19(4) ISSA Journal 12-15.
[41]Jianhua, 'The economic impact of cyber terrorism' [2013] 22(2) Journal of strategic information system 175-186.
[42] ibid.
[43]Arul, E., Punidha, A. (2021). Adware Attack Detection on IoT Devices Using Deep Logistic Regression SVM (DL-SVM-IoT). In: Sharma, H, Saraswat, M, Yadav, A, Kim, J.H, Bansal, J.C. (eds) Congress on Intelligent Systems. CIS 2020. Advances in Intelligent Systems and Computing, vol 1334. Springer, Singapore https://doi.org/10.1007/978-981-33-6981-8_14.

i. **Structured query language injection:** A Structured query language injection (SQL) injection attack installs malicious code into a SQL-using server to manipulate a database.[44]
j. **Man-in-the-middle (MITM) attack:** MITM attacks include hackers interfering with a two-person internet transaction. Once inside, the hackers may sift and grab data. MITM attacks are frequently carried out on insecure public Wi-Fi networks.[45]

2.3. Benefits of Cybersecurity

Today, cyber security sector is largely concerned with defending devices and systems from attackers. While the bits and bytes driving these efforts might be difficult to visualize, the implications are much easier to consider.[46] Many websites would be practically impossible to enjoy if cyber security specialists did not work ceaselessly to prevent denial-of-service attacks.[47] Without strong cyber security measures, it would be relatively easy to destroy modern-day necessities such as electricity systems and water treatment plants that keep the globe operating smoothly. Simply put, cyber security is critically important because it helps to preserve the lifestyles we have come to know and enjoy.[48]

2.4. Fundamentals of Cybersecurity

As technology advances, cyber-attacks evolve as attackers grow more creative, making it critical for individuals and organizations to correctly describe and comprehend cyber security principles.[49] A model

[44]Justine Clarke, SQL Injection Attacks and Defense (2nd edn, Syngress 2012).
[45]AvijitMallik, 'MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORD' [2018] 2(2) Cyberspace 109-134.
[46]ZuopengJustinzhang and others, 'Cybersecurity awareness training programs: a cost–benefit analysis framework' [2021] 131(3) Emerald insight 613-636.
[47] ibid.
[48] ibid.
[49]Dave clemente, Fundamentals of cyber security. in Larry macfaul (ed), VERIFICATION & IMPLEMENTATION A biennial collection of

architecture that aids organizations in developing their security policies includes three key concepts: confidentiality, integrity, and availability. It is sometimes referred to as the CIA Triad.[50]

Let's look at some key Cybersecurity ideas that are intended to ensure the safety of each component.

a. **Confidentiality:** Data is the most significant source of information for every organization, and safeguarding its secrecy is a top concern.[51] The goal of confidentiality is to keep data from being disclosed to unauthorized parties.[52]Basic notions of confidentiality in cyber security include aiming to keep the identities of authorized parties involved in data transfer and storage private and anonymous. Most of the time, breaking inadequately encrypted data, man-in-the-middle (MITM) attacks, and revealing sensitive data compromise secrecy.To guarantee secrecy, data encryption, biometric verification, security tokens, and two-factor authentication are used.[53]These methods can alter how data is handled inside an organization and maintain data security.[54]
b. **Integrity:** It is also vital for the organization to maintain data consistency, correctness, and dependability over time, which is accomplished through integrity, which prevents data from being updated by unauthorized parties.[55]Additionally, data should not be modified, altered, destroyed, or viewed unlawfully while being sent. Changes to the program and information must be

analysis on international agreements for security and development (3G Evolution Ltd 2015) 177.

[50] ibid.

[51]P Jain and others, 'Big data privacy: a technological perspective and review' [2015] 3(25) Journal of big data 16-59.

[52] ibid.

[53] ibid.

[54] ibid.

[55]Venkatesakumar and G Poornima, 'Ensuring Data Integrity in Cloud Computing' [2012] 5(4) Journal of Computer Applications 1-8.

made in an approved manner. Turning a workstation into a "zombie computer" and injecting malware into web pages are two acknowledged threats to integrity. Cryptographic checksums, file permissions, uninterrupted power supply, and data backups are some typical ways to ensure integrity.[56]Along with basic safeguards, instruments and technology that may identify changes or breaches in data must be incorporated. Different applications employ checksums and cryptographic checksums used by different organizations to verify the integrity of the data.[57]

c. **Availability:** According to this fundamental cyber security idea, authorized parties must have access to information whenever it is required.[58]Data is only valuable if the appropriate people have access to it at the appropriate time. To ensure that the data is available and accessible when needed, it must be stored in a secure environment.[59]All relevant components, including as hardware, software, networks, and devices, should be maintained and upgraded to provide smooth data access.Unavailability of information can occur as a result of security incidents such as DDoS (distributed denial-of-service) attacks, hardware problems, code flaws, and human errors.Some basic steps to ensure availability include firewalls, data backup to external drives, data redundancy, and backup power supply.[60]Availability is not just about data but also about having total cybersecurity for your organization; it should have additional security equipment available in case of a disaster or limitation in data access.[61]

[56] ibid.
[57]ibid.
[58]Von Solmsrossouw and Johan van niekerk, 'From information security to cyber security' [2013] 38(13) Elsevier 97-102.
[59] ibid.
[60] ibid.
[61] ibid.

3.0 Cybercrime Laws

Cybercrime law establishes standards of conduct and behavior for the use of the Internet, computers, and related digital technologies, as well as the actions of public, government, and private organizations; rules of evidence and criminal procedure, as well as other criminal justice matters in cyberspace; and regulation to reduce risk and/or mitigate the harm done to individuals, organizations, and infrastructure in the event of a cybercrime.[62] As a result, cybercrime law encompasses substantive, procedural, and preventative law.

3.1. Statutory Law

An unlawful conduct must be specifically defined and forbidden by law. A person cannot be punished for an act that was not prohibited by law at the time the conduct was performed, according to the moral principle of *nullum crimen sans lege* (Latin for "no crime without law").[63] Substantive law establishes the rights and obligations of legal subjects, which include individuals, organizations, and governments. Statutes and ordinances established by local, state, and federal legislatures (statutory law), federal and state constitutions, and court judgments.[64]

3.1.2 Substantive cybercrime legislation comprises statutes that ban particular forms of cybercrime and penalize non-compliance. Cybercrime encompasses both traditional, real-world (offline) crimes (e.g., fraud, forgery, organized crime, money-laundering, and theft) committed in cyberspace as 'hybrid' or 'cyber-enabled' crimes and 'new' or 'cyber-dependent' crimes made possible by the Internet and Internet-

[62]OlusolaMaitanmi and others, 'Cyber Crimes and Cyber Laws in Nigeria' [2013] 2(4) The International Journal Of Engineering And Science 19-25.
[63]Thomas J Holt and others, 'Regulating Cybercrime through Law Enforcement and Industry Mechanisms' [August 2018] 679(1) AAPSS 551.
[64] ibid.

enabled digital.[65] For these reasons, numerous nations have enacted legislation aimed primarily at combating cybercrime, Germany, Japan, and China, for example, have altered pertinent portions of their penal codes to tackle cybercrime.[66] Countries have also leveraged existing laws created for offline (real-world) crime to pursue certain cybercrimes and cybercriminals.[67] In Iraq, for example, the existing civil law (Iraqi Civil law No. 40 of 1951) and penal code (Iraqi Penal Code No. 111 of 1969) are utilized to punish real-world crimes committed via the Internet and digital technologies (e.g., fraud, blackmail, identity theft).[68]
Substantive law focuses on the ingredients of a crime, such as the illegal activity (actusreus - "guilty act") and the mental aspect (mensrea - "guilty mind").[69] Countries may prosecute the same behavior, but their laws may differ as to what "state of mind" renders people accountable for their actions (i.e., level of criminal culpability).[70] To that purpose, regulations that prohibit, for example, unlawful access to computer systems and data differ among nations, depending on the level of intent held by the alleged criminal.[71]

3.1.3 Criminal liability levels

[65]John OlayemiOdumesi, 'Combating the Menace of Cybercrime' [2014] 3(6) International Journal of Computer Science and Mobile Computing 980-991.
[66] ibid.
[67]iIbid.
[68]MazenIsmaeelghareb and Falah Mustafa sedeeq, 'Electronic Crimes And The International Community Legislation: Comparative Analytical Study' [August 2018] 7(8) International Journal of Scientific & Technology Research 175-180.
[69]Paul Robinson, Should the Criminal Law Abandon the Actus Reus-Mens Rea Distinction? in P Robinson (ed), The Structure and limits of criminal law (Routledge 2017) 26.
[70] ibid.
[71]R E Bell, 'The Prosecution of Computer Crime' [2002] 9(4) Journal of financial crime 308-325.

The degree to which an illicit act was intentional (purposefully or wilfully committed) or unintentional (recklessly and negligently committed) varies according to legal system.[72]When a person acts with the intent to do harm, that person is committing a crime on purpose.[73] The United Kingdom Computer Misuse Act of 1990, for example, criminalizes illegal access to systems and data with the goal of causing alterations or damage, disruptions of systems and services, and modifications of system data and programs.[74]

A person commits a deliberate crime when he or she is aware that an activity will cause harm but still conducts the harm or wrongdoing. Individuals conduct crimes carelessly when they participate in an act while being aware of the considerable and unreasonable danger of damage to others yet demonstrate contempt for or indifference to the risk of harm.[75]

In Australia, a person can be charged under the Cybercrime Act 2001 (No. 161, 2001) if the "person is reckless as to whether the [unauthorized] modification [of data] impairs or will impair: (i) access to that or any other data held in any computer; or (ii) the reliability, security, or operation, of any such data."[76]

The lowest level of guilt is negligence. Those that engage in irresponsible behaviour are unaware of the harmful effects of their actions. Anyone who even through negligence, processes or arranges the processing of personal data without having complied with the formalities set out in the Law on Personal Data prior to using such data shall be punished".[77]

---

[72]L Ivanova, 'Criminal Liability for Cybercrimes in the BRICS Countries' [2023] 10(1) BRICS Law Journa 59-87.

[73] ibid.

[74]Computer Misuse Act of British Parliament 1990.

[75] ibid.

[76]477.2(1)(c) Cyber Crime Act of Australia.

[77]M Daniel Filler and others, 'Negligence at the breach: Information fiduciaries and the duty to care for data' [2022] 54(1) Heinonline 105.

3.2 Procedural Cybercrime Law

Procedural law defines the processes and procedures that must be followed in order to apply substantive law, as well as the norms that must be followed in order for substantive law to be enforced.[78] Criminal procedure is an important part of procedural law because it includes comprehensive rules and guidelines on how suspected, accused, and convicted persons are to be handled and processed by the criminaljustice system and its agent.[79]Finally, procedural cybercrime legislation comprises regulations on jurisdiction and investigative authorities, evidence rules, and criminal process pertaining to data collection, eavesdropping, search and seizure, data preservation, and data retention.[80]

3.2.1 Jurisdiction and Investigative Authorities under Cybercrime

Law enforcement may conduct cybercrime investigations only if the interested state has jurisdiction, and national courts may only hear cybercrime matters if the interested state has jurisdiction.[81] The power and authority of a state to enforce laws and penalize disobedience with laws is referred to as jurisdiction.[82] State sovereignty, defined as a country's power to exert control over its own territory, is connected to jurisdiction.[83] Geographic territory or *locus commissi deliciti* (the site where the crime was done) is usually related with jurisdiction, wherein states claim jurisdiction over and prosecute crimes committed inside

[78]Ladan M, 'Legal Regimes on Cyber Crimes and Electronic Evidence in Nigeria and Africa' [2020] SSRN Electronic Journal.

[79] ibid.
[80] ibid.
[81]Brown Cameron, 'Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice ' [June 2015] 9(1) International Journal of Cyber Criminology 55-119.
[82]Dorsett Shaunnagh , Jurisdiction (1st edn, Routledge 2012) 10.
[83] ibid (pg 12).

their territory (principle of territoriality). Because cyberspace lacks geographic boundaries and territories, geography cannot be utilized to define jurisdiction.[84]As a result, governments rely on a variety of additional elements to determine. One such aspect is the offender's nationality (principle of nationality; active personality principle). According to this notion, governments have the ability to punish its citizens even if they are outside of their territory. To a lesser degree (in its application), the victim's nationality can be utilized to establish jurisdiction over a crime (principle of nationality; passive personality principle).[85] A state may also establish jurisdiction if a crime committed in another state (for example, treason or espionage) has harmed the interests and security of the state seeking jurisdiction over the case (protective principle). Finally, when the state where the crime was committed is unwilling or unable to prosecute the offender (principle of universality), any state can establish jurisdiction over certain transnational crimes, such as mass atrocities (e.g., genocide), which are viewed as affecting all human beings regardless of geographic location.[86]

3.2.2 Investigative Powers and Measures.

Cybercrime digital evidence offers unique issues in terms of management and usage in judicial processes.[87] According to the 2013 UNODC Draft Comprehensive Study on Cybercrime, "[while some of these investigative actions can be accomplished using traditional powers, many procedural provisions do not translate well from a spatial, object-oriented approach to one involving...[digital] data storage and real-time data flows", necessitating the use of specialized powers for the

[84]ibid.
[85] ibid.
[86] ibid.
[87]Sun Jia-rong and others, 'A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure' [2015] 17(5) International Journal of Network Security 497-509.

investigation. These specialized capabilities are established by law and contain safeguards to guarantee that data is collected in accordance with valid legal orders and accessed only to the degree required and allowed by law.[88]

A governmental entity may require the disclosure of the contents of a wire or electronic communication that has been electronically stored in an electronic communications system for one hundred and eighty days or less by a provider of electronic communication service only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.[89] These precautions (i.e., the demand for legal order) are, however, not required by all governments. Turkey revised Internet Law 5651 in 2014 to oblige Internet service providers to store user data and make it available to authorities upon request without first needing them to get a legal order (e.g., a court order or search warrant).[90]

3.2.3 Issues relating to Digital Evidence and Cybersecurity

The identification, gathering, storing, analyzing, and disseminating of digital evidence are all covered by cybercrime procedural legislation. Any type of information that may be retrieved from computers or other digital devices and used to support or refute the existence of an offense is referred to as digital evidence (also known as electronic evidence).[91] Digital evidence has the power to confirm or deny the veracity of claims made by victims, witnesses, and suspects, as well as to pinpoint the

[88]Jan-Jaapoerlemans, Investigating cybercrime (2nd edn, Amsterdam University Press 2017) 20.

[89]SabillonRegner and others, 'Digital Forensic Analysis of Cybercrimes: Best Practices and Methodologies' [2017] 11(2) International Journal of information and security privacy 13.

[90]ibid.

[91]Molina Granja Fernando and others, 'The preservation of digital evidence and its admissibility in the court' [2017] 9(1) International journal of electronic securities and digital forensics 1-18.

whereabouts and intentions of the perpetrator as well as his or her past behaviors and behavior.[92]

The standards used to establish whether digital evidence is admissible in court are governed by the rules of evidence and criminal procedure. To ensure that digital evidence is admissible in national courts, these guidelines specify how it should be recorded, gathered, communicated, analyzed, kept, and protected.[93] Digital evidence must be validated and have its integrity shown in order to be acceptable. Identification of the source/author of the digital evidence and confirmation of the evidence's integrity (i.e., that it was not altered, manipulated, or damaged in any way) are both steps in the authentication process.[94] To ensure that digital evidence is admissible in the majority of legal proceedings, it is crucial to maintain a chain of custody, a detailed log about the evidence, its state, collection, storage, access, and transfer, as well as the reasons for those accesses and transfers (UNODC, 2013, p. 54; Maras, 2014). Criminal procedure and evidence laws vary from one nation to the next. Because cybercrime crosses international borders and affects digital devices and systems everywhere there is an Internet connection, similar norms of proof and criminal procedure are required.[95]

3.3 Preventative Cybersecurity Laws

Regulation and risk reduction are the main goals of preventive law. Preventive law in the context of cybercrime aims to either stop it from happening or, at the very least, lessen the harm that results from it. As discussed in Cybercrime Module 10 on Privacy and Data Protection, data protection laws (such as the EU General Data Protection Regulation of 2016 and the African Union Convention on Cybersecurity and

[92]ibid.
[93] ibid.
[94]Olivier Leroux, 'Legal admissibility of electronic evidenceFootnote1he preservation of digital evidence and its admissibility in the court' [2007] 18(4) International review of law computers and technology 193-220.
[95]ibid.

Personal Data Protection of 2014) and cybersecurity laws (such as The Law of Ukraine on the Basic Principles of Ensuring the Cybersecurity of Ukraine of 2017) are intended to lessen the tangible harms from criminal breaches of personal data should a cybercrime occur, and/or to prevent such harms from occurring.[96]

By ensuring that the necessary resources, controls, and procedures are in place to make these actions possible (such as ensuring that the infrastructure of telecommunications and electronic communications service providers permits wiretapping and data preservation), other laws help criminal justice professionals identify, investigate, and prosecute cybercrime. The Communications Assistance for Law Enforcement Act (CALEA) of 1994 in the United States required telecommunications service providers and equipment manufacturers to make sure that their services and products allow government agencies with legitimate authorization (i.e., the proper legal order) to access communications.[97]

4.0. Cybercrime Laws in Nigeria

4.1 Evidence Act, 2011: this act talks about the admissibility of electronic evidence.[98] The Cybercrime (Prohibition, Prevention, Etc) Act, 2015 outlines the procedural powers and rules for cybercrime investigations and the gathering of electronic evidence of a criminal offense.[99]

A person who knowingly or intentionally sends a message or other item through computer systems or a network that is grossly

[96]Nunes ED, 'United Nations Office on Drugs and Crime (UNODC). Global Study on Homicide: Trends, Context, Data. Vienna: UNODC; 2011' (2012) 17 Ciência& SaúdeColetiva 3447.

[97] M. Harbawi and A. Varol, 'An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework', 2017 5th International Symposium on Digital Forensic and Security (ISDFS), TirguMures, Romania, 2017, pp. 1-6, doi: 10.1109/ISDFS.2017.7916508.

[98] Sections 84 and 258 of the Evidence Act 2011.

[99] Section 24 of the Cybercrime (prohibition, prevention ETC) Act 2015.

offensive, pornographic, or otherwise of an indecent, obscene, or menacing nature, or causes any such message or item to be sent, or he knows to be false, with the intent to annoy, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will, or needless anxiety is in violation of the Act.[100]

4.2Data Protection Act 2023

The Data Protection Act of 2023 was enacted into law on June 14 by President Bola Ahmed Tinubu.[101] Protecting fundamental freedoms and rights as well as the interests of data subjects as established by the Nigerian Constitution of 1999 is one of the Act's goals.[102]

4.1 Legal Framework for Cyber Security in Nigeria

4.1.1 Cybercrime Act 2015

This is the first legislation that deals with Cybersecurity. Passed in May 2015, it gives effect to 2011 ECOWAS Directives on fighting crimes in the sub-region. The Act charges the offices of National Security Advisor and Attorney-General of the Federation.[103]

4.1.2 Criminal Code Act, 1990

Although cybercrime is not specifically listed in the Act, it is crime under the Criminal Code. The act discusses gaining property under false pretenses.[104] The act also deals with crime.[105]The act clearly defines what constitutes an offense under the statute.[106]

4.1.3 Advance Fee Fraud and other related offenses Act 2006

[100]ibid.
[101] The Data Protection Act 2023.
[102] ibid.
[103] The Cybercrime (prohibition, prevention ETC) Act 2015.
[104] Chapter 4 of the Criminal Code Act CAP38 LFN 2004.
[105] Section 419 0f the Criminal Code Act CAP38 LFN 2004.
[106]Section 418 0f the Criminal Code Act CAP38 LFN 2004.

Although advance fee fraud has been around since the 13th century, the current version first appeared in the 1920s. Its primary focus is on frauds involving Africans, particularly Nigerians.[107] The most common term used is "419 fraud." According to the law, anyone who obtains something from someone else for themselves or another person under false pretenses and with the intent to defraud, or who induces someone else to deliver something to someone else, or who obtains anything else, whether or not the thing is obtained or its delivery is induced through the use of a contract induced by false pretense, violates the Act.[108]

4.1.4 The Economic and Financial Crime Commission Act of 2004

The creation of the commission is outlined in the Act. Its primary duties include:

Investigating all financial crimes, such as advance fee fraud, money laundering, forging documents, transferring funds illegally, and future market funds, etc.

The commission is also charged with the duty of enforcing the requirements of the Money Laundering Act 1998.

The commission is further charged with the coordination and enforcement of all laws against economic and financial crime legislation and enforcement functions granted to any other person and authority.[109]

4.1.5 National Cyber Security Framework of NITDA, 2014

The National Cybersecurity Framework was created in 2014 by Nigeria's National Information Technology Development Agency (NITDA). The framework is intended to give Nigerian Cybersecurity challenges a strategic perspective. In order to improve the nation's Cybersecurity posture, it describes the standards, regulations, and practices that government entities, businesses, and other stakeholders must follow.[110]

---

[107] Advanced Fee Fraud and other Related Offences Act CAPA6 LFN 2004.

[108] ibid.

[109] The Economic and Financial Crimes Commission Act CAPE1 LFN 2004.

[110] Godwin Thomas and Mary-Jane Sule, 'A service lens on cybersecurity continuity and management for organizations' subsistence and growth' [2022] 3(1) *Organisational Cybersecurity Journal* 18-40.

The National Cybersecurity Framework is designed to protect sensitive data, safeguard key information infrastructure, and lessen cyber threats. It also offers a base for developing a safe online environment in Nigeria.[111]

5.0 Cyber Security Myths and Misbelieves

We are well aware of the growing number of cyber-attacks. Organizations and people must safeguard themselves against the majority of risks in the modern technological era. Unfortunately, there are still a few Cybersecurity myths that discourage far too many individuals from taking the required steps to protect their personal information.[112]

5.1 Here are some Cybersecurity myths one should know

a. **Passwords are enough:**You can protect yourself by using passwords alone, but you shouldn't rely exclusively on passwords to protect your data. Even though secure passwords are crucial, hackers may still find a method to crack them. As a result, it's essential to put in place strong Cybersecurity procedures and a multilayered defense. [113]
b. **Removing the file from the computer**: This action sends the file to the Recycle Bin, where it is eventually deleted. Data that has been deleted still exists on the hard disk, for instance in the temporary files folder.[114]

[111]ibid.
[112]ibid.
[113]JaiswalManishaben , 'Cybercrimes Categories and Prevention' [2019] 7(1) SSRN 526-536.
[114]Singh Vinay and others, '"Efficacy of open source tools for recovery of unconventionally deleted data for forensic consideration"' [2015] 3(9) International Journal of Social Relevance & Concern 53-59.

c. **Encryption solutions are not worthwhile**: Some businesses continue to hold the belief that they don't need encryption software. The idea that encryption will stop data intrusions is untrue. In order to protect oneself from fraudsters and ransomware assaults, encryption is essential.[115]
d. **Small and medium-sized enterprises are not targeted**: It is a fallacy to believe that only large corporations lack adequate security and are hence the only ones that cybercriminals target. Sixty-one percent of all small and medium-sized organizations reported experiencing at least one cyber-attack in the past year, according to the 2021 Data Breach Investigations Report. Due to the weaker security measures used by these businesses. Therefore, it is essential to safeguard businesses against cybercrime.[116]

5.2 Key Cybersecurity Technologies and Best Practices

Here is a given best practices list one should follow:[117]

a. Use VPN to privatize your connections, before clicking on links check the links
b. do not be lethargic with your passwords,
c. Scan external devices for viruses,
d. store sensitive information in a secure place,
e. enable two-factor authentication,
f. double-check the HTTPS on websites,
g. remove adware from the computer,
h. disable Bluetooth connection when you are not using it,

[115]Rasori Macro and others, 'A Survey on Attribute-Based Encryption Schemes Suitable for the Internet of Things' [2022] 9(11) IEEE Internet of Things Journal 8269-8290.
[116]Paolo bellavista, 'Machine Learning Cybersecurity Adoption in Small and Medium Enterprises in Developed Countries' [2021] 10(11) MDPI 150.
[117]William Stallings , Effective Cybersecurity: A guide to using best practices and standards (Pearson 2019) 28.

i. avoid using public networks,
j. invest in security upgrades and employ white hat hacker

6.0 Conclusion

It is generally known that challenges precede growth.[118] These challenges might be both natural and man-made.[119] Criminals have a highly fruitful environment to carry out their evil activities because of the advent of technology and the internet.[120] As a result, an assessment of cyber security and cybercrime in Nigeria reveals a complex cyber ecosystem riddled with both obstacles and possibilities.[121] The recent digitalization of many areas of the economy has undoubtedly brought numerous benefits, but it has also exposed the country to an endless stream of cyber-attacks.[122]

Individuals, organizations, and the government are all at danger from cybercrime, which includes phishing, ransomware, and other criminal actions.[123] To address cybersecurity challenges in Nigeria, a succinct and coordinated strategy is required. To establish and execute effective Cybersecurity frameworks, regulations, and procedures, policymakers, law enforcement agencies, and the commercial sector must

[118]Dhiman Bharat, 'Key Issues and New Challenges in New Media Technology in 2023: A Critical Review' [2023] 5(1) Journal of Media & Management 1-4.
[119] ibid.
[120]Mostafa al-emran and Griffy-Brown Charla , 'The role of technology adoption in sustainable development: Overview, opportunities, challenges, and future research agendas' [2023] 73(12) Elsevier 102.
[121]Ebenezer Akpan, 'A Strategic Assessment of Cyber Security Strategies and Mitigation of Cybercrime in Nigeria' [2019] 5(3) GASPRO Intl Journal of Eminent Scholars 1-15.
[122] ibid.
[123]Sulaimanabdul-rasheed and others, 'Cybercrime and Nigeria's External Image: A Critical Assessment' [August 2016] 9(6) Africology: The Journal of Pan African Studies 119-132.

collaborate.[124] It is critical to invest in Cybersecurity education and awareness initiatives that will equip individuals and companies to protect themselves against growing cyber threats.[125]

The paper also emphasizes the importance of noting that cyber threats transcend national borders, and effective strategies necessitate global collaboration. International cooperation in the fight against cybercrime in Nigeria, sharing information and cutting-edge practices to improve its Cybersecurity capabilities is a welcome idea.

The problem is a continuum, and the investigation finds good aspects such as the growth of Cybersecurity firms and improved company awareness. These considerations give Nigeria with a chance to boost its Cybersecurity posture and establish itself as a regional Cybersecurity leader.[126]

To summarize, combating Cybersecurity and cybercrime in Nigeria necessitates a multifaceted approach that incorporates technology improvements, regulatory measures, and concerted efforts from all parties. As a result of taking immediate action, Nigeria reduces the risks associated with cyber-attacks while simultaneously fostering a safe digital environment favorable to economic growth and creativity.

7.0 Recommendations

This paper poses the following recommendations

i. Legislative enhancements: there should be a periodic review and updating of the existing Cybersecurity laws to match the evolving threats landscapes. Also, amendments to combats emerging challenges in the cyber world
ii. Public-private partnership: Platforms for collaborative efforts between public and private cyber users should be

[124] ibid.
[125] ibid.
[126] ibid.

enabled. This will form a formidable force that can withstand the threats in the cyber ecosystem.

iii. Empowering law enforcement agents: Apart from equipping them with up-to-date gadgets, they should be trained on the latest cyber security practices available in the developed world, since most of the criminals are well trained and are ever updating on new technological flaws in cyber security trends.

iv. Continuous Monitoring and evaluation: Controls should be put in place for monitoring and evaluation of the success and failures of the Cybersecurity in place. This mechanism should be constants review to add the changing trends to the security and policies in place.

v. Strengthening international collaborations: International aids should be in place among the enforcement agencies. Facilitate partnership with cyber-advance nations to learn and seek assistance where necessary.